UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

TERRY MONSKY, Individually and On Behalf of All Others Similarly Situated, Plaintiff, vs. DIRECT DIGITAL HOLDINGS, INC., MARK WALKER, KEITH W. SMITH, DIANA DIAZ, and DIRECT DIGITAL MANAGEMENT, LLC, Defendants.	Case No. 4:24-cv-01940 (Consolidated with Case No. 4:24-cv-02567) Judge Kenneth M. Hoyt

APPENDIX OF EXHIBITS IN SUPPORT OF LEAD PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

Lead Plaintiff Donald W. Hutchings, by and through undersigned counsel, respectfully submit this Appendix in support of his opposition to Defendants' Motion to Dismiss (ECF 44).

APPENDIX A

INDEX OF EXHIBITS

EX.	DOCUMENT	DATE	APP. PAGE #
	Declaration Of Michael I. Fistel, Jr. in Support of Lead Plaintiff's Opposition to Defendants' Motion to Dismiss	March 14, 2025	Pl. Appx. A-001–002
A-1.	"Tinder Lets Known Sex Offenders Use the App. It's Not the Only One," *ProPublica* article	December 2, 2019	Pl. Appx. A-003–032
A-2.	Second Amended Class Action Complaint for Violations of the Federal Securities Laws filed in *Crutchfield v. Match Grp., Inc., et al.,* No. 3:19-cv-02356 (N.D. Tex.).	April 23, 2021	Pl. Appx. A-033–197
A-3.	Order on Defendants' Motion to Dismiss Second Amended Complaint filed entered in *Crutchfield v. Match Grp., Inc., et al.*, No. 3:19-cv-02356 (N.D. Tex.).	November 19, 2021	Pl. Appx. A-198–200

DATED: March 14, 2025

JOHNSON FISTEL, LLP

/s/ Michael I. Fistel, Jr.

Michael I. Fistel, Jr.
Attorney-In-Charge
Murray House
40 Powder Springs Street
Marietta, GA 30064
Telephone: (470) 632-6000
Facsimile: (770) 200-3101
michaelf@johnsonfistel.com

JOHNSON FISTEL, LLP
Jeffrey A. Berens
2373 Central Park Boulevard, Suite 100
Denver, CO 80238-2300
Telephone: (303) 861-1764
jeffb@johnsonfistel.com

Lead Counsel for Plaintiff and the Class

SPONSEL MILLER PLLC
Thane Tyler Sponsel III (Texas SBN 24056361)
Federal ID No. 690068
520 Post Oak Blvd.
Houston, TX 77027
Telephone: (713) 892-5400
sponsel@smglawgroup.com

Local Counsel for Plaintiff and the Class

CERTIFICATE OF SERVICE

The undersigned hereby certifies that all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF system on March 14, 2025.

/s/ Michael I. Fistel, Jr.
MICHAEL I. FISTEL, JR.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

TERRY MONSKY, Individually and On Behalf of All Others Similarly Situated, Plaintiff, vs. DIRECT DIGITAL HOLDINGS, INC., MARK WALKER, KEITH W. SMITH, DIANA DIAZ, and DIRECT DIGITAL MANAGEMENT, LLC, Defendants.	Case No. 4:24-cv-01940 (Consolidated with Case No. 4:24-cv-02567) Judge Kenneth M. Hoyt

DECLARATION OF MICHAEL I. FISTEL, JR.
IN SUPPORT OF LEAD PLAINTIFF'S OPPOSITION
TO DEFENDANTS' MOTION TO DISMISS

Under 28 U.S.C. § 1746, I, Michael I. Fistel, Jr., declare as follows:

1. I am a partner at Johnson Fistel LLP, Lead Counsel for Lead Plaintiff Donald W. Hutchings in the above-styled action.

2. I am legally competent to make this declaration. I have personal knowledge and am familiar with the matters stated in this declaration, and the facts contained herein are true and correct.

3. Attached as Exhibit A-1 is a true and correct copy of an article titled "Tinder Lets Known Sex Offenders Use the App. It's Not the Only One" from *ProPublica*, dated Dec. 2, 2019, which is attached as Exhibit 4 to the excerpt of the Appendix of Exhibits in Support of Defendants' Motion to Dismiss in *Crutchfield v. Match Grp., Inc., et al*., No. 3:19-cv-02356 (N.D. Tex.).

4. Attached as Exhibit A-2 is a true and correct copy of the Second Amended Class

Action Complaint for Violations of the Federal Securities Laws filed on April 23, 2021 in *Crutchfield v. Match Grp., Inc., et al*., No. 3:19-cv-02356 (N.D. Tex.).

5. Attached as Exhibit A-3 is a true and correct copy of the Order on Defendants' Motion to Dismiss Second Amended Complaint filed entered on November 19, 2021 in *Crutchfield v. Match Grp., Inc., et al.*, No. 3:19-cv-02356 (N.D. Tex.).

I declare under the penalty of perjury that the foregoing is true and correct.

Executed this 14th day of March 2025 in Marietta, Georgia.

MICHAEL I. FISTEL, JR

EXHIBIT A-1

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

PHILLIP R. CRUTCHFIELD, Individually and On Behalf of All Others Similarly Situated, Plaintiff, v. MATCH GROUP, INC., AMANDA W. GINSBERG and GARY SWIDLER, Defendants.	§ § § § § § § § § § § § § §	Civil Action No. 3:19-cv-2356

APPENDIX OF EXHIBITS IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS

Defendants Match Group, Inc. ("Match Group"), Amanda W. Ginsberg, and Gary Swidler, by and through undersigned counsel, respectfully submit this Appendix in support of their Motion to Dismiss.

INDEX OF EXHIBITS

EX.	DOCUMENT	DATE	APP. PAGE(S)
	Declaration of Peter A. Stokes, Esq.	6/12/2020	1-4
1	Match Group Form 10-K (2017)	3/1/2018	5-127
2	Match Group Form 10-K (2018)	2/28/2019	128-248
3	*Match Responds to FTC Lawsuit*, Press Release	9/25/2019	249-251
4	"Tinder Lets Known Sex Offenders Use the App. It's Not the Only One," *ProPublica* article	12/2/2019	252-276
5	Match Group Form 10-K (2019)	2/27/2020	277-421
6	Match Group Stock Price Chart	6/12/2020	422-429
7	NASDAQ Index Chart	6/12/2020	430-447
8	*Match Group Reports Third Quarter 2018 Results and Announces Special Dividend*, Press Release	11/6/2018	448-461
9	Q3 2018 Earnings Call Transcript	11/7/2018	462-482
10	*Match Group Reports Fourth Quarter and Full Year 2018 Results*, Press Release	2/6/2019	483-494
11	Q4 and FY 2018 Earnings Call Transcript	2/7/2019	495-514
12	*Match Group Reports First Quarter 2019 Results*, Press Release	5/7/2019	515-526
13	Q1 2019 Earnings Call Transcript	5/8/2019	527-546
14	Match Group Form 10-Q (Q1 2019)	5/9/2019	547-606
15	*Match Group Reports Second Quarter 2019 Results*, Press Release	8/6/2019	607-618
16	Q2 2019 Earnings Call Transcript	8/7/2019	619-637
17	Match Group Form 10-Q (Q2 2019)	8/8/2019	638-688
18	*Match Group Reports Third Quarter 2019 Results*, Press Release	11/5/2019	689-700

EX.	DOCUMENT	DATE	APP. PAGE(S)
19	Q3 2019 Earnings Call Transcript	11/6/2019	701-718
20	Match Group Form 10-Q (Q3 2019)	11/7/2019	719-771

Dated: June 12, 2020

Respectfully submitted,

NORTON ROSE FULBRIGHT US LLP

/s/ *Peter A. Stokes*

Gerard G. Pecht (Attorney-in-Charge)
State Bar No. 15701800
1301 McKinney, Suite 5100
Houston, TX 77010-3095
Telephone: (713) 651-5151
Facsimile: (713) 651-5246

Peter A. Stokes
State Bar No. 24028017
peter.stokes@nortonrosefulbright.com
98 San Jacinto Boulevard, Suite 1100
Austin, Texas 78701-4255
Telephone: (512) 474-5201
Facsimile: (512) 536-4598

Robert Greeson
State Bar No. 24045979
Lead Attorney
robert.greeson@nortonrosefulbright.com
2200 Ross Avenue, Suite 3600
Dallas, Texas 75201
Telephone: (214) 855-7430
Facsimile: (214) 855-8200

Counsel for Defendants

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing document was filed with the Court's electronic case filing (ECF) system on June 12, 2020, which caused an electronic copy of this document to be served on all counsel of record in this matter who have registered for ECF service.

/s/ *Peter A. Stokes*
Peter A. Stokes

Exhibit 4

Tinder Lets Known Sex Offenders Use the App. It's Not the Only One.

Match Group, which owns most major online dating services, screens for sexual predators on Match — but not on Tinder, OkCupid or PlentyofFish. A spokesperson said, "There are definitely registered sex offenders on our free products."

Pl. Appx. A-009

by Hillary Flynn, Keith Cousins and Elizabeth Naismith Picciani, Columbia Journalism Investigations, Dec. 2, 2019, 5 a.m. EST

App. 253

Above: Nicole Xu, special to ProPublica

ProPublica is a nonprofit newsroom that investigates abuses of power. Sign up to receive our biggest stories as soon as they're published.

This article is co-published with Columbia Journalism Investigations and BuzzFeed.

Susan Deveau saw Mark Papamechail's online dating profile on PlentyofFish in late 2016. Scrolling through his pictures, she saw a 54-year-old man, balding and broad, dressed in a T-shirt. Papamechail lived near her home in a suburb of Boston and, like Deveau, was divorced. His dating app profile said he wanted "to find someone to marry."

Deveau had used dating websites for years, but she told her adult daughter the men she met were "dorky." She joked about how she could get "catfished" if a date looked nothing like his picture. Still Deveau, 53, wanted to grow old with someone. The two were — in the popular dating platform's jargon — "matched."

A background check would have revealed that Papamechail was a three-time convicted rapist. It would have shown that Massachusetts designated him a dangerous registered sex offender. So how did PlentyofFish allow such a man to use its service?

PlentyofFish "does not conduct criminal background or identity verification checks on its users or otherwise inquire into the background of its users," the dating app states in its terms of use. It puts responsibility for policing its users on users themselves. Customers who sign its service agreement promise they haven't commited "a felony or indictable offense (or crime of similar severity), a sex crime, or any crime involving violence," and aren't "required to register as a sex offender with any state, federal or local sex offender registry." PlentyofFish doesn't attempt to verify whether its users tell the truth, according to the company.

Papamechail didn't scare Deveau at first. They chatted online and eventually arranged a date. They went on a second date and a third. But months after their PlentyofFish match, Deveau became the second woman to report to police that Papamechail raped her after they had met through a dating app.

PlentyofFish is among 45 online dating brands now owned by Match Group, the Dallas-based corporation that has revenues of $1.7 billion and that dominates the industry in the U.S. Its top dating app, Tinder, has 5.2 million subscribers, surpassing such popular rivals as Bumble.

For nearly a decade, its flagship website, Match, has issued statements and signed agreements promising to protect users from sexual predators. The

site has a policy of screening customers against government sex offender registries. But over this same period, as Match evolved into the publicly traded Match Group and bought its competitors, the company hasn't extended this practice across its platforms — including PlentyofFish, its second most popular dating app. The lack of a uniform policy allows convicted and accused perpetrators to access Match Group apps and leaves users vulnerable to sexual assault, a 16-month investigation by Columbia Journalism Investigations found.

Match first agreed to screen for registered sex offenders in 2011 after Carole Markin made it her mission to improve its safety practices. The site had connected her with a six-time convicted rapist who, she told police, had raped her on their second date. Markin sued the company to push for regular registry checks. The Harvard-educated entertainment executive held a high-profile press conference to unveil her lawsuit. Within months, Match's lawyers told the judge that "a screening process has been initiated," records show. After the settlement, the company's attorneys declared the site was "checking subscribers against state and national sex offender registries."

After Match connected Carole Markin with a six-time convicted rapist, she sued the company to push for regular registry checks. (Kendrick Brinson for ProPublica)

The next year, Match made similar assurances to then-California Attorney General Kamala Harris. In a 2012 agreement on best industry practices between the attorney general's office and the dating site, among others, the company again agreed to "identify sexual predators" and examine sex offender registries. It pledged to go further and respond to users' rape complaints with an additional safety tool: "a rapid abuse reporting system."

Today, Match Group checks the information of its paid subscribers on Match against state sex offender lists. But it doesn't take that step on Tinder, OkCupid or PlentyofFish — or any of its free platforms. A Match Group spokesperson told CJI the company cannot implement a uniform screening protocol because it doesn't collect enough information from its free users — and some paid subscribers — even when they pay for premium features. Acknowledging the limitations, the spokesperson said, "There are definitely registered sex offenders on our free products."

CJI analyzed more than 150 incidents of sexual assault involving dating apps, culled from a decade of news reports, civil lawsuits and criminal records. Most incidents occurred in the past five years and during the app users' first in-person meeting, in parking lots, apartments and dorm rooms. Most victims, almost all women, met their male attackers through Tinder, OkCupid, PlentyofFish or Match. Match Group owns them all.

In 10% of the incidents, dating platforms matched their users with someone who had been accused or convicted of sexual assault at least once, the analysis found. Only a fraction of these cases involved a registered sex offender. Yet the analysis suggests that Match's screening policy has helped to prevent the problem: Almost all of these cases implicated Match Group's free apps; the only service that scours sex offender registries, Match, had none.

In 2017, Tinder matched Massachusetts registered sex offender Michael Durgin with a woman, and she later told police he had raped her on their first date; Durgin's two rape charges were dropped after the woman "indicated that she does not wish for the Commonwealth to proceed to trial," records show. (Durgin didn't respond to requests for comment.) OkCupid allowed another registered sex offender, Michael Miller, of Colorado, to create a new account after his 2015 conviction for raping a woman he met through the site. For months, Miller remained on the platform despite appearing on the registries Match screens. Even Pennsylvania registered sex offender Seth Mull, whose 17-year history of sex crimes convictions began as a teen, used Match Group's dating sites; in 2017, PlentyofFish didn't flag his eight-year registry status before matching him with a woman who later accused him of rape. Mull is now serving life in prison for her rape and two more rapes, among other sex crimes.

Asked about the CJI data, Match Group's spokesperson said the 157 cases "need to be put in perspective with the tens of millions of people that have used our dating products."

The company declined multiple requests to interview executives and other key employees familiar with its protocols for addressing online dating sexual assault. The spokesperson described the steps the company takes to ensure customer safety on its platforms — from blocking users accused of sexual assault to checking across its apps for accused users' accounts and

flagging them on a companywide distribution list. Other response protocols aren't standardized across Match Group apps.

In a brief statement, the company said it "takes the safety, security and well-being of our users very seriously." Match Group said "a relatively small amount of the tens of millions of people using one of our dating services have fallen victim to criminal activity by predators." It added, "We believe any incident of misconduct or criminal behavior is one too many."

Interviews with more than a dozen former Match Group employees — from customer service representatives and security managers at OkCupid to senior executives at Tinder — paint a different picture. Most left on good terms; indeed, many told CJI they're proud of the successful relationships their platforms have facilitated. But they criticize the lack of companywide protocols. Some voice frustration over the scant training and support they received for handling users' rape complaints. Others describe having to devise their own ad hoc procedures. Often, the company's response fails to prevent further harm, according to CJI interviews with more than 100 dating app users, lawmakers, industry experts, former employees and police officers; reviews of hundreds of records; and a survey of app users.

Even the screening policy on the one site that checks registries, Match, is limited. The company's spokesperson acknowledges that the website doesn't screen all paid subscribers. The site has argued in court for years that it has no legal obligation to conduct background checks, and it fought state legislation that would require it to disclose whether it does so.

Markin, whose civil suit led to the registry policy, cannot help but feel the company has failed to deliver. Calling registry screenings "the easiest kind of cross-checking," she said she had expected Match Group to embrace the practice.

"I did something to help other women," she told CJI. "It's disappointing to see Match did not."

Susan Flaherty grew up in the 1960s outside Hoboken, New Jersey, where she developed a style that her daughter describes simply as "Jersey": "big-haired, blonde, blue-eyed and loud." With a head for numbers, she got a degree in finance and spent most of her adult life working as a mortgage broker.

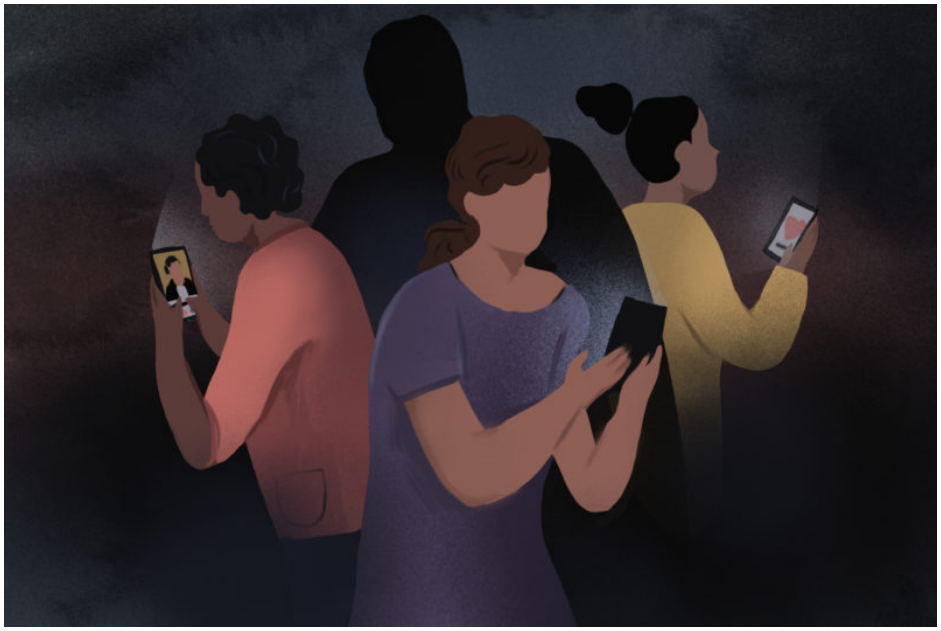
In the mid-1990s, she walked into a bar near Naples, Maine, and came face to face with Denie Deveau, a bartender. They got married and had two children. Seven years later, they divorced. Susan kept her husband's last name. She bounced from relationship to relationship after that. She always thought she "needed a man to come take care of her," her 24-year-old daughter, Jackie, said.

Papamechail grew up in the 1960s in Peabody, Massachusetts, just north of Boston. He came from a prominent family that owns a construction company. Since the late 1980s, Papamechail has built a rap sheet consisting of eight criminal convictions, four of them sex crimes. He has pleaded guilty to three separate rapes.

His first rape conviction in 1987 involved a neighbor and resulted in an eight-year prison sentence and a 10-year probationary period "with special conditions to undergo sex offender treatment." Court records show Papamechail served one year in prison and later violated his probation. Within four years, he was convicted of rape again for two more incidents. During that case, he told police he had a "problem" and needed "help," court records show. He spent another four years behind bars. By 1994, he had spent yet another year in prison after his second conviction for indecent assault and battery, a sex crime in Massachusetts. Court records show Papamechail has served a total of at least eight years in prison. The state officially designated him a sex offender.

Papamechail declined to comment for this article. He told a CJI reporter over Facebook that "if you ever contact me or my family again I will reach out to the Massachusetts courts."

In 2014, Papamechail became familiar to sex crimes detectives again. This time, a woman he met through PlentyofFish accused him of raping her on their first date. The claim put him in county jail without bail for two years; he was eventually acquitted after a weeklong jury trial. Still, law enforcement officials raised his sex offender status to the state's most dangerous category, Level III, deeming him highly likely to offend again.



Nicole Xu, special to ProPublica

By the time PlentyofFish matched him with Deveau, Papamechail's heightened status meant he would have already appeared on the state's sex offender registry — something that PlentyofFish didn't check, the company confirms. At the time, Deveau, a recovering alcoholic, was living in a sober house near Papamechail's home. Over the ensuing months, the pair chatted online. They texted and spoke on the phone. They met in person; she went to his apartment twice.

Then, in October 2017, Papamechail picked up Deveau for what would be their final date, court records show. They went for dinner and returned to his home. She "expected to just hang out together," court records note she told the grand jury, but he had "other plans." They got into a fight. "He wanted her in the bedroom," according to her testimony, "but she said no." Around 7:40 p.m., court records show, she called the Peabody emergency dispatch service for help.

Deveau told the 911 dispatcher "a man was trying to rape her and had threatened her," the court records state. "He's coming," she told the dispatcher, dropping the phone.

Susan Deveau is among the users in CJI's data who reported being victimized by someone they met through a dating platform. The analysis suggests the problem has grown as the popularity of online dating has soared — in 2015, 12% of American adults were on a dating site, compared with 3% in 2008. Other studies reinforce this trend. In 2016, the U.K. National Crime Agency reviewed police reports over a five-year period and found online-dating sexual assault had increased as much as 450% — from 33 to 184 cases.

Because no one collects official statistics on online dating sexual assault in the U.S., CJI surveyed more than 1,200 women who said they had used a dating platform in the past 15 years. It is a non-scientific questionnaire about an underreported crime, and the results represent only CJI's specific group. They are not generalizable and cannot be extrapolated to all online dating subscribers. (Read the survey's methodology at the end of this story.) Among this small group, more than a third of the women said they were sexually assaulted by someone they had met through a dating app. Of these women, more than half said they were raped.

If such results are confirmed by further studies, the numbers would be alarming, said Bethany Backes, an assistant professor in the Violence Against Women Faculty Cluster Initiative at the University of Central Florida. Backes, who reviewed CJI's questionnaire, noted that this one group of dating app users reported a higher rate of sexual assault than women in the general population do. Backes speculated that's because the

users sampled were actively dating. The results, she added, suggest a need for the platforms to protect their users not just online but offline as well.

"I think anyone has a moral responsibility to do something about it," Backes said, "whether they think they have a legal or business responsibility."

Match Group declined to comment on CJI's survey. Its spokesperson noted that Match Group CEO Mandy Ginsberg has prioritized customer safety. "I'm a woman and a mom of a 20-year-old who uses dating apps," the executive said in an interview in 2018 with The Wall Street Journal. "I think a lot about the safety and security, in particular, of our female users."

In 2018, Ginsberg launched a safety council made up of leading victim advocates and other experts. Interviews with its members show that the council has focused on getting users to take action themselves rather than having the company act.

Match has long argued that such checks were too incomplete or costly for its users. Markham Erickson, a lawyer specializing in internet law who worked with Match to lobby against background checks, told CJI it was "incredibly hard" to screen online dating users. "It's not like you're getting the fingerprint of an individual," he said. All a sex offender "had to do was give a false name."

A Match Group spokesperson contends that background checks do little more than create what she calls "a false sense of security" among users. "Our checks of the sex offender registry can only be as good as the information we receive," she said, explaining that the government databases can lack data, have old pictures or include partial information on sex offenders.

But some in the industry have argued that the onus should be on the dating app companies to check users' backgrounds to protect their customers from predators. Herb Vest, a Texas entrepreneur who made a legislative crusade out of the issue in the 2000s, launched his own dating platform in 2003. Dubbed True.com, the company's name reflected its policy of screening users for sex crimes and other felonies, Vest said. It paid approximately $1 million a year for third-party services like rapsheets.com and backgroundchecks.com, partly because public registries were scattershot at first, and partly because the vendors could do a more comprehensive check.

The contracts allowed the company to screen an unlimited number of subscribers each month, former True president Reuben Bell said, an expense it incorporated into membership fees totaling $50 a month. By contrast, Match charged a similar monthly rate — $60 at the time — without conducting any form of background check.

True even warned subscribers that the company would sue if they misrepresented their pasts. “If you are a felon, sex offender or married, DO NOT use our website,” it stated on its site. In 2005, the company took one registered sex offender to court after discovering he had lied about his status. The lawsuit settled. According to Vest, the man agreed to stop using dating platforms. True ultimately folded in 2013.

Another Match Group rival, a free dating app called Gatsby that operated from 2017 until this year, used government databases to screen its 20,000 users. Gatsby’s founder, Joseph Penora, told CJI in an email he was inspired to create what he calls “a creepy guy filter” after reading about a woman who was assaulted by a sex offender she had met through Match. “Our users are the backbone of our success,” Penora wrote. “Let’s do something proactive to keep them safe.”

Even former Match Group insiders agree the registries are more accessible and have fewer blind spots today. Several former security executives told CJI that such screenings would be a feasible way to help prevent online dating sexual assault — if the company invested the resources. For example, they and other experts say Match Group, which expects to make around $800 million in profits this year by one measure, could purchase an application program interface, or API, from a third-party vendor to allow it to check its users against the nearly 900,000 registered sex offenders in the U.S.

Vest still cannot understand why the industry has resisted such measures. He insists the cost of doing background checks didn’t play a role in his company’s closing. True’s bankruptcy records blame its subscription losses on banking reforms after the recession that left consumers with limited or no credit.

The company’s background-checking policy wasn’t mentioned in the thousands of pages of filings. Nor did True report owing money to its screening vendors.

“People can’t rely 100% on the sites,” Vest said. “But as an industry, we could have done much better.”

Peabody police officers responded to Deveau’s 911 call on Oct. 28, 2017, arriving at a multifamily complex with a purple door. The officers found her and Papamechail outside, court records show. There, she told the police that he had demanded sex. When she refused, she said, he pushed her against the wall and yelled, “I am going to have you one way or another.”

Peabody police had come there before. In March 2014, Janine Dunphy reported that Papamechail had raped her at his home after the two had

met through PlentyofFish, which Match Group would buy within the year.

Janine Dunphy at her family cabin. In 2014, Dunphy reported that Mark Papamechail, a registered sex offender, had raped her at his home after the two had met through PlentyofFish. Dunphy saw Papamechail back on the app in 2016. (Sarah Rice, special to ProPublica)

Dunphy's allegations sounded strikingly similar to those of Deveau, court records show. Both said he invited them to his home after a date. When they refused his sexual advances, their victim testimonies state, Papamechail — he is 6 feet, 2 inches tall and weighs 260 pounds, according to the state sex offender registry — threw them on the floor or the bed, restrained them with his arms and raped them.

Papamechail pleaded not guilty to Dunphy's rape charge; at the 2016 trial, his defense attorney claimed the incident was consensual and questioned the influence of her medical prescriptions and financial motivations. "Her story changes," his lawyer said at the time. "And the truth never changes."

Dunphy never knew Papamechail was a registered sex offender when PlentyofFish had matched them, she said. During the criminal case, she told a detective that Papamechail had confided that he was kicked off the Match dating site but didn't say why, the police report shows. Match Group declined to confirm or deny whether its flagship platform has ever blocked Papamechail. Prosecutors tried to subpoena PlentyofFish for records of his correspondence with her. Dunphy remembers that the company, which is based in Canada, refused, saying it didn't have to comply with U.S. subpoenas.

By 2016, the registry board had raised Papamechail's sex offender status to the highest level, indicating what the board considers "a high degree of danger to the public." Papamechail's listing, including a photo, appeared on the registry's public website, where it remains today. The

Massachusetts board declined to comment on Papamechail's sex offender history, citing state laws.

"He's going to do it over and over again," said Dunphy, who has a lifetime restraining order barring Papamechail from contacting or abusing her. In the winter of 2016, she remembers seeing him back on PlentyofFish, which by then was owned by Match Group.

Ten months later, the Peabody detective responded to the 911 call at Papamechail's house. Deveau reported he had raped her in a follow-up interview. "She did not tell police on the date of the incident because she stated she was afraid and she wanted to leave," court records note. By January 2018, a grand jury had found enough evidence to indict him for rape. Papamechail pleaded not guilty. He told police that he and Deveau had been in an off-and-on sexual relationship. He maintained that he didn't try to have sex with Deveau, and that she "woke up abruptly and was screaming at him, calling him a sex offender and a rapist," the police report states.

In a February 2018 decision ordering his temporary detention as a "habitual offender," Superior Court Judge Timothy Feeley ruled that Papamechail's "propensity for sexual violence against women is uncontrollable." The judge found that "even house arrest would not in this court's view protect future potential victims of Papamechail's sexual violence." One of the reasons Feeley cited was Papamechail's online activities.

Papamechail stands out among the convicted and alleged perpetrators in CJI's data. Most dating app users accused of assaulting another user weren't registered sex offenders at the time. Some had past sex crime convictions. Others were subjects of prior police complaints. But most of the time checking users' criminal backgrounds alone would not have prevented the problem, the analysis found.

Match Group presents its rapid abuse reporting system as crucial for protecting customers from sexual assault. "Our brands also depend on our users to report any profiles engaged in concerning behavior so that we can investigate and take appropriate action," the company states on its website. Any user can log a complaint online or through its apps. Moderators and security agents try to identify the accused user and block his account, according to the company. They check across platforms for other associated accounts.

"If there's bad behavior on one app," Match Group CEO Ginsberg has said, describing the company's response protocols, "we can identify that user, we'll kick him off all the apps."

But some users who reported their rape claims to the company describe a different outcome. Brittney Westphal, 31, who lives outside Aspen, Colorado, said she informed Tinder in 2015 that another user had raped her on their first date. She asked the dating app how she could get a record of her conversations with the accused when he "unmatched" her — which instantly deletes the history of communication between two users — leaving her unable to give his information or a record of their conversations to police.

Tinder never replied, she said, and local authorities declined to press charges. "I made it clear to them [Tinder] like how serious this was," Westphal said, "and then I never heard anything." Within months, she said she spotted her alleged attacker on the app again.

A Utah college student, Madeline MacDonald, told Tinder in a December 2014 email that she "was sexually assaulted (or something very similar)," records show. She provided the app with pertinent information, including the accused's name, age and physical description. The next day, their email correspondence shows, a Tinder employee asked for screen shots of his app profile, adding that a link to the accused's Facebook profile "could help as well." MacDonald offered screenshots of his Facebook page, which included his employer, town, high school and phone number. An employee responded by asking for a link to the Facebook page. MacDonald said she gave up. Eventually, she said she saw her alleged assailant back on Tinder.

Three years later, according to Dixie State University Police Chief Blair Barfuss, a detective in his unit informed MacDonald that the man she had accused had allegedly assaulted three other women he met through dating apps. Two were Match Group platforms.

And then there's Kerry Gaude, 31, of Golden, Colorado, whose experience after Michael Miller raped her on their first date illustrates the shortcomings of Match Group's protocols. When OkCupid matched the two in May 2014, Miller, then 28 and using the handle mike22486, was not yet a registered sex offender. Two women who had met him online told police he sexually assaulted them, but their claims didn't lead to criminal charges. Gaude reported her rape to police, and then she emailed OkCupid and PlentyofFish. She remembers warning the platforms that a rapist was using their services to meet women.

Kerry Gaude was raped by Michael Miller after the two met on OkCupid. Miller pleaded guilty to sexual exploitation and assault charges. Gaude said she frequently saw Miller on OkCupid after the sentencing. (Rachel Woolf for ProPublica)

The following year, Miller pleaded guilty to sexual exploitation and assault charges stemming from Gaude's claim. He got 10 years' probation with sex offender stipulations prohibiting him from using "any applications to communicate with women in any way about sex," court records state. He also appeared on the state's public sex offender registry two days after his sentencing in May 2015, state officials confirm.

Yet Gaude said she frequently saw Miller on OkCupid after the sentencing. Within three months, in fact, he was charged with probation violations after admitting to using an unapproved cellphone to access the app, records show. The violations put him in a Cañon City, Colorado, prison for four years.

During the proceedings, Gaude went on local TV and warned people that Miller could victimize other OkCupid users.

Three women contacted police about their exchanges with Miller on the dating app throughout 2015. Police records show one 25-year-old got a message on OkCupid from a man with the handle lucky4me123. On his profile, the man presented himself as an "independent yet naturally caring" person who lived alone and hoped to "find that special someone." He was, OKCupid said, a "67% match" in compatibility for the woman. She recognized Miller's mugshot from a news article about Gaude's warnings.

By then, Miller had been listed in the state's online sex offender database for almost seven months. The Colorado bureau that administers the registry had no record of Match Group employees requesting information about individuals on its offender list during this time. A Match Group spokesperson confirms OkCupid never checked his registry status.

"It's the after the fact that bothers me," Gaude said of Miller's ability to keep using OkCupid. "How is that not aiding and abetting?"

Match Group's spokesperson said the company uses "industry-leading automated and manual moderation and review tools," and spends millions every year to "prevent, monitor and remove people who engage in inappropriate behavior from our apps."

Several former OkCupid employees familiar with the company's complaint process say it is easy for banned individuals, like Miller, to get back on the app. The company's moderators adopt a general "ban first" mentality for any accused user, the employees said, but once blocked, they have little ability to stop the accused from using different identifying information, or signing up for new accounts. Some say they complained about this issue to OkCupid supervisors, only to be ignored. Others say they found themselves searching public offender lists on their own.

Match Group, for its part, declined to comment.

Miller didn't respond to repeated interview requests, and nobody answered the door when a CJI reporter visited his house. While on probation, Miller wrote to one woman on OkCupid, apologizing for his crime and pleading for "the opportunity to prove myself that im not a bad indiviual."

Now on parole, he is subject to intensive supervision. One condition prohibits him from using online dating sites.

Some time after Deveau had reported her rape allegation to police, her daughter, Jackie, remembers being on a lunch break when she got a phone call from the assistant district attorney handling the Papamechail criminal case. Her mother had returned to drinking by then, Jackie said, and shut herself off from family.

Jackie knew her mother had experienced something bad with a date, but she didn't know anything more until a prosecutor told her. She recalls hearing Papamechail's litany of sex crime convictions. Still on the phone, Jackie looked him up on the internet and scrolled through news articles on Dunphy's case. She learned about his registry status. "It was just horrifying," Jackie said.

Jackie dialed her mother right away. Deveau sounded drunk and incoherent, so Jackie didn't broach the criminal case. Her mother's behavior seemed to be unraveling from the ordeal, Jackie said.

In April 2018, Jackie got another phone call about her mother. This time, she learned Deveau was in the hospital, admitted after a drinking binge,

her vitals unstable. Jackie arrived at the hospital; within days, doctors were putting her mother on life support.

Deveau died on April 27, 2018, from "acute kidney failure," her death certificate states.

By May, the Middlesex County District Attorney's Office was forced to drop the criminal case it was building against Papamechail. It filed a formal notice ceasing prosecution on two counts of rape, citing Deveau's death. "Without the testimony of the alleged victim in this sexual assault case," it stated in its filing, "the Commonwealth is unable to meet its burden at trial to prove the defendant guilty beyond reasonable doubt."

Papamechail was released from jail again but remained on the state's registry. Once again, he would be spotted on a Match Group app.

When Jackie learned her mother had met Papamechail through PlentyofFish, she considered suing. The dating app could have prevented what happened, she said, especially considering "how severe he is as a sex offender." Intimidated by the well-resourced company, she never did file a civil lawsuit.

Even if Jackie had gone to court, though, the Communications Decency Act would have rendered legal action practically futile. The act, passed in 1996, when internet companies were nascent and viewed as needing protection, contains a provision, known as CDA Section 230, that was originally intended to protect websites from being held liable for their users' speech.

Companies, including Match Group, have successfully invoked CDA 230 to shield themselves from liability in incidents involving users harmed by other users, including victims of sexual assault. Internet regulation experts say the measure effectively allows online dating companies to avoid legal repercussions. In the few civil suits accusing Match Group platforms of negligence for online dating sexual assaults, its lawyers have cited CDA 230 to try to dismiss nearly every one, records show.

Olivier Sylvain, a Fordham University law professor who specializes in the ethics of media and technology, believes judges have been so overly generous in interpreting CDA 230 that they dismiss cases before an aggrieved party can even obtain information about the company's response. "That speaks to how these companies are held unaccountable," he said.

Only one civil suit, filed against Match in an Illinois county courthouse in 2011, has gotten around CDA 230. The case ended in an undisclosed settlement in April 2016. Over its five-year history, it pried open internal

Match documents shedding light on how the site has handled online dating sexual assault.

Nicole Xu, special to ProPublica

The case dates back to December 2009, when Match connected Ryan Logan, then 33, a Chicago technology consultant, with a 31-year-old baker identified as Jane Doe. The woman, whose name has never been made public, asked to remain anonymous for this article. She told police Logan had raped her on their first date, spurring a chain of events that would lead him to be convicted of sexual assault in 2011. Around the time of his criminal trial, she learned another woman had previously accused Logan of rape and had alerted Match.

Logan "proceeded to date rape me," the woman wrote the site in a 2007 complaint. She warned Match he could use its service to attack others.

Logan didn't respond to multiple requests for comment for this article. Currently an Illinois registered sex offender, he was ordered to pay more than $6 million in damages to Doe as a result of her civil suit. The judge in his criminal case barred Logan from using online dating services.

Company documents obtained during the discovery process show Match's customer service team treated the sex assault complaint as it would any other at the time: It sent the complaint to a security agent, who created an incident case file. But Match's response ended there. "The employee who was to handle the case did not follow internal procedure and closed the case without taking action," the documents state. The site didn't take down Logan's profile at the time, nor did it acknowledge the woman's complaint.

During the civil proceedings, Match attempted to dismiss the negligence claims, citing CDA 230. In December 2013 — a year after it promised to implement registry screenings and response protocols — the dating site used the law to argue against any obligation to remove users who become subjects of sex assault complaints.

"Whatever Match does, whether they leave the profile on or take it off, even if they had knowledge, is a protected act," James Gardner, its lawyer, claimed in court. He maintained the site shouldn't be responsible for taking action against accused users even if it failed to remove a user after being warned about him. "Why shouldn't they be responsible for that?" Gardner asked rhetorically. "The law says they are not. And the reason the law says they are not is because we understand that the larger purpose of internet commerce is more important."

Circuit Court Judge Moira Johnson rejected that argument, finding "the allegations do not support conduct that is immune" under CDA 230, which covers third-party content, a hearing transcript states.

Discovery documents offered a rare window into Match's response system. As of November 2007, court filings show, the site was keeping track of users accused of sexual assault in a spreadsheet detailing their identification numbers, handles and full names. The site handed over nearly 1,300 complaints of physical and sexual violence filed by users against other users during the two years preceding Doe's rape. The judge ruled the spreadsheet's contents could be redacted and the complaints sealed, making it impossible to glean whether or not Match could identify repeat offenders among its subscribers and, if so, how it responded.

Match Group declined to comment on the redacted spreadsheet's numbers, or to release its own numbers of sex assault complaints filed with its apps.

Doe thought Match executives would be outraged that an accused rapist had been allowed back on their site, she said, but she soon learned otherwise. The site discouraged her from speaking publicly about her case, and it has yet to implement her policy recommendation for a user assault hotline. The Match Group spokesperson notes the company's safety pages list support services for sex assault victims. But the company doesn't sponsor its own hotline for its users.

Its lawyers pointed out in court records that Match's "common sense recommendations" for offline user conduct advise never meeting in a private location. "We're not going to say, 'Oh my gosh, it was her fault that he raped her," Gardner said during a hearing, "but she has to take some responsibility."

Doe still tears up when she remembers how Match treated her in court. "You are not a victim," she told CJI. "You are enemy No. 1."

Janine Dunphy had learned, through a local newspaper article in early 2018, that Papamechail had allegedly assaulted another woman whom he met through a dating app. Then, in May last year, Dunphy got a phone call from an assistant district attorney, the same one who had handled the case involving Papamechail and Dunphy. "I have some really bad news," she recalls the prosecutor saying. The woman had died. The rape charges had been dropped.

The news sent Dunphy on a quest to find Papamechail on PlentyofFish. She had made fake profiles to try to track him down on the platform before. She created a male profile once and posted some of his photos alongside warnings of his sex-offender status to see if the website would react. Another time she used a fake female profile without pictures to see if the app would connect them. Sometimes, she searched for his dating profiles for hours.

"I lost so much of my life," said Dunphy, whose health has deteriorated in the years since her rape claim. Doctors have diagnosed her with blood clots from stress, therapists have treated her for post-traumatic stress disorder. Of her Papamechail date, she said, "It's in my head every day."

Dunphy said she continued to see Papamechail on PlentyofFish until she stopped searching last fall. (Sarah Rice, special to ProPublica)

Dunphy recalls finding his profile on PlentyofFish less than a month after she had heard about Deveau's death. She recognized Papamechail's pictures — a photo of himself in a car, another of an orange cat. His username was Deadbolt56. He described himself as a "coffee snob." She took screenshots of his profile, she said, and notified PlentyofFish. She never heard back.

Match Group would not confirm or deny whether PlentyofFish ever received a complaint about Papamechail. Its spokesperson said the company's team of security agents removed him from its platforms more than a year ago — around the time Dunphy would have filed her complaint — but didn't answer questions about why he was barred, how many times he's been barred or how often he's gotten back on the apps. According to Match Group, there are no accounts associated with Papamechail on its platforms.

Dunphy said she continued to see him on PlentyofFish until she stopped searching last fall. She got tired of trying to keep Papamechail off the site, she says. She felt like she was doing the work the app should've been doing.

Over the past 15 years, as online dating has emerged as the most popular matchmaker among Americans, state legislators have tried to address its potential for real-world harm. The earliest proposals would have required platforms to conduct full background checks. But since online dating companies do business nationwide, and only the federal government can regulate interstate operations, they went nowhere.

State lawmakers then took a different tack and pushed to mandate that apps disclose whether or not they conduct background checks. These laws, typically enforced by state attorneys general or consumer affairs departments, fine companies if they don't disclose. These measures explain why Match Group platforms adopted the no-check warnings buried in their Terms of Use in the first place.

In 2005, legislators — from Virginia to California, and Michigan to Florida — were debating disclosure bills championed by True.com. Vest, True's founder, considered the company's legislative campaign a form of marketing that would inspire brand loyalty. Generally opposed to government intervention, he saw an exception in this case. "We have a legislative branch intended to protect the citizenry," Vest said.

Among the most vocal critics of the bills was Match. In Michigan, for example, Marshall Dye, then assistant general counsel for the website, testified at a hearing on that state's bill. Match opposed the bill, Dye testified, on the grounds that it would give users a false sense of security. Consumers might assume that everyone on the platform had a spotless record, she argued. But no one convicted of a crime would give his real name. (Dye declined a request to comment on her testimony.)

"It's just a buyer beware statement," said Alan Cropsey, a Michigan state senator at the time who sponsored the failed bill because he figured industry support would be a no-brainer. Of the platforms, he said, "They don't want the buyer to beware."

New Jersey became the first state in 2008 to pass an online dating disclosure statute, which also required the platforms to publish safety tips — such as "Tell friends and family about your plans," and "Meet in public and stay in public." Legislatures in Illinois, New York and Texas soon followed suit. At times, Match lobbyists led the industry opposition in the debates.

Match Group didn't soften its stance until 2017, when the company helped to push a measure that would lead to California's first — albeit limited — online dating rules. State lawmakers say the #MeToo movement's momentum drove passage of provisions that require dating platforms to offer California users the same safety tips and reporting processes already required elsewhere. The regulations don't mandate any form of background check.

Today, just five states have regulations aimed at improving online dating customer safety. Records requests filed in those states have yielded hundreds of complaints about the industry involving contract disputes or romance scams. None involve online dating sexual assault. No state regulators have taken action against a platform for violating disclosure rules.

Former Texas State Sen. Leticia Van de Putte, who sponsored that state's 2011 legislation, said states can only do so much to protect dating app users. "We really do need to have some sort of national framework," she said.

Last May, Jackie sat in a conference room at her employer's office in Portland, Maine, taking in a photograph of Deveau. It was three weeks after the first anniversary of her mother's death, and her grief was palpable. "I need my Mom more than anything," she wrote on her Facebook page weeks earlier. The photograph in her hand depicts Jackie as an infant, sitting in Deveau's lap. Jackie, sucking on her mother's finger, wears an oversized floppy pink hat. Deveau wears a wide grin.

Jackie remembers small moments growing up with her mother: a look the two would share when a snack craving overcame them. Deveau would drive Jackie to a local convenience store to order big salted pretzels. Or the pool parties her mother hosted at their home, where she always put out a good spread and welcomed everyone with open arms.

Deveau spoke constantly on the phone with Jackie as an adult — until she stopped.

Jackie wore a V-neck striped shirt, a tattoo peeking out from underneath. It depicts the jagged line of a heart monitor before Deveau's last heartbeat. Jackie got it etched over her own heart to commemorate her mother.

Reflecting on her mother's last months, Jackie portrayed Deveau like so many women who use online dating apps: vulnerable, at risk of assault. She doubted Deveau would have thought about registry screenings and response protocols. She finds it "disgusting" that online dating companies like Match Group would expect its female users to check sex offender lists themselves.

They may be looking for the man of their dreams on these dating apps, Jackie said, but they "can't do that if these predators are on there."

Share Your Story

Name *

Email *

What would you like to tell us about? *

- I used a dating service and have a story to tell.
- I have a story from a friend or family member who used a dating service.
- I am or was an employee or contractor for Match or another dating service.
- I work in law or law enforcement and have insight into how such reports are handled.
- Other

Do you have documents (emails, PowerPoint presentations, memos, spreadsheets, etc.) that highlight what you're sharing with us? If so, we would love to see them. You can upload them here or get in touch with us at datingapps@propublica.org

UPLOAD A FILE

State of residence

Alabama

City or town of residence

Thanks so much for your help. The more examples we can verify, the better our reporting will be. We hope to compile enough examples to potentially share with dating app companies, in order to to bring any patterns we find to their attention. If that happens, can we use your story in our dataset with identifying information redacted?

- Yes
- No
- Please talk to me first

OUR COMMITMENT TO YOUR PRIVACY

We appreciate you sharing your story and we take your privacy seriously. We are gathering these stories for the purposes of our reporting, and will not share your information with third-parties without your express permission.

NOTE: A journalist in our reporting network may be in touch with further questions.

We may have follow-up questions. What's the best way to reach you?

- ☐ Email
- ☐ Phone
- ☐ Either email or phone
- ☐ Other

Select all that apply

What time of day tends to work best for you?

- ☐ Morning
- ☐ Afternoon
- ☐ Evening
- ☐ It doesn't matter
- ☐ Other

Select all that apply

SPREAD THE WORD.

Thank you for sharing with us. Help us reach as many people as possible in order to better understand this topic.

How did you find this form? I saw it on/in:

- ☐ ProPublica
- ☐ Columbia Journalism School newsletter or social media
- ☐ Buzzfeed News
- ☐ Facebook
- ☐ Twitter
- ☐ Reddit
- ☐ Instagram

- [ ] Someone sent it to me directly
- [ ] An article
- [ ] A ProPublica newsletter
- [ ] Another forum, newsletter, blog, group I subscribe to
- [ ] Other

Do you have ideas for getting the word out? Who else should we talk to?

Do you want to be notified when ProPublica publishes big investigations? *

- (•) Yes
- ( ) No

Saved SUBMIT

Powered by Screendoor.

Methodology

Columbia Journalism Investigations worked with subject matter experts primarily at Columbia University — from public health researchers to sociologists and statisticians — to craft and vet our questionnaire for dating app users. No government agency in the United States has data on online dating sexual violence, and the questionnaire was meant to initiate a larger reporting effort, bringing us leads and directions to follow. It is not a formal survey. Respondents were not selected at random from a population but instead volunteered to fill in the questionnaire. For that reason, we do not claim that our results represent the general experience of dating app users.

We relied on the online survey platform Amazon Mechanical Turk (MTurk) to distribute an initial questionnaire to identify women living in the U.S. who had used an online dating site over the past 15 years. Some researchers have used this platform to ask participants — who receive compensation for their time — about traumatic events and experiences. Following MTurk's guidelines, we made our questionnaire available to

potential respondents in all regions of the country, and we screened out anyone who had a poor record of taking questionnaires.

In all, 2,151 women responded to the initial questions establishing that they live in the U.S. and have used dating apps. Of these, 1,244 volunteered to complete our full questionnaire. Our questions included general inquiries into demographic information, online dating experiences and consensual sexual behavior. Respondents also answered five questions meant to describe acts of sexual assault and rape. These questions, developed in consultation with our experts, followed professional standards for sexual violence surveys. We eliminated results that could be classified as "bad data," such as those from people who started but did not finish the questionnaire.

Overall, 31% of the women in the survey reported being sexually assaulted or raped by someone they had met through an online dating site.

Our database of incidents of sexual assault involving online dating platforms was created from a web scrape of a decade of news reports and civil lawsuits that CJI reporters vetted and analyzed. Most of the 157 cases took place during the past five years. We then corroborated these cases through court and police records, as well as interviews with officials and additional media reports.

We want to learn more about what actions dating platforms are and are not taking when users report episodes of sexual violence. We need to collect as many stories as possible for further reporting.

If you or someone you know has reported an incident to Match, OKCupid, Tinder, or any other dating app, please fill out our confidential survey.

If you or someone you care about has been affected by sexual assault and would like confidential help and support, please call the National Sexual Assault Hotline at 800-656-4673 to talk to a trained staff member from a nearby sexual assault service provider.

Hillary Flynn, Keith Cousins and Elizabeth Naismith Picciani are reporting fellows for Columbia Journalism Investigations, an investigative reporting unit at the Columbia Journalism School. CJI research assistant Andrea Salcedo contributed reporting to this story. Funding for CJI is provided by the school's Investigative Reporting Resource and the Stabile Center for Investigative Journalism.

EXHIBIT A-2

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

PHILLIP R. CRUTCHFIELD, Individually and On Behalf of All Others Similarly Situated,

Plaintiff,

v.

MATCH GROUP, INC., AMANDA W. GINSBERG, and GARY SWIDLER,

Defendants.

Case No.: 3:19-cv-02356

SECOND AMENDED CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS

JURY TRIAL DEMANDED

TABLE OF CONTENTS

Co-Lead Plaintiffs, Phillip R. Crutchfield and Samir Ali Cherif Benouis ("Plaintiffs"), individually and on behalf of all other persons similarly situated, by their undersigned attorneys, for their complaint against Defendants, allege the following based upon personal knowledge as to themselves and their own acts, and information and belief as to all other matters, based upon, *inter alia*, the investigation conducted by and through their attorneys, which included a review of Defendants' public statements and publicly available documents, conference calls and announcements, SEC filings, wire and press releases published by and regarding Match Group, Inc. ("Match Group" or "Match"), analysts' reports and advisories and other press coverage about Match, Match's stock chart, Match's corporate website, data obtained through news services such as Bloomberg and Yahoo! Finance, interviews with certain confidential witnesses ("CWs") who were former employees of Match and the brands it owns, information obtained through Freedom of Information Act requests, and information readily obtainable through publicly available sources and on the Internet. Plaintiffs believe that substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

I. NATURE OF THE ACTION

1. This is a federal securities class action brought on behalf of a class consisting of all persons and entities who purchased or otherwise acquired the common stock of Match Group, Inc. (NASDAQ: MTCH) between November 6, 2018 and January 31, 2020, both dates inclusive ("Class Period"), seeking to pursue remedies against Match and certain of its officers and/or directors named as Defendants herein for violations of the federal securities laws under the Securities Exchange Act of 1934 (the "Exchange Act").

2. Match Group operates a suite of dating and matchmaking websites and applications ("apps") accessed through computers and devices, including popular brands like Match.com,

Tinder, PlentyofFish. It derives substantially all its revenues from payments by a portion of its registered members, those it can convert from a free or trial membership to a premium or paid membership, like Tinder Gold. To gauge its success, Match tracks financial and performance metrics that are publicly reported to analysts and investors, including its "paid member count" or "PMC", the conversion rate from unpaid to paid memberships, and the average revenue per user (or "ARPU"), in addition to more traditional reporting metrics like revenues and earnings.

3. Unbeknownst to investors, Match's websites and apps suffered from rampant levels of scammers, "bots," and other fraudulent accounts among its registered users, a "significant" percentage of whom paid premiums for access to enhanced features, both to avoid detection and as a prerequisite to accessing the features and functionalities necessary to carry out their scams. These nefarious actors sought to extract money or things of value from Match's legitimate customers. Worse, most of Match's brands also failed to screen for sex offenders and other dangerous users, leading to a high number being on those sites. These underlying, negative, undisclosed facts were described by numerous CWs, all former employees of Match Group or its branded websites and apps like Tinder and Match.com. They describe a 15% to 20% rate of fraudulent accounts on these Match websites/apps. They also describe how this percentage of fraudulent accounts, if stable, was simply assumed, such that company forecasts were not adjusted to exclude those accounts, even those that were paid subscriptions.

4. Investors also did not know the extent to which Match understaffed and impeded its own anti-fraud efforts. The CWs speak of small Fraud Department teams of just eight people tasked with manually identifying and making removal decisions on millions of potentially fraudulent accounts, in high volume and at high speed. The CWs described how the company failed to implement touted technological anti-fraud measures and how cost concerns dictated that

anti-fraud personnel head counts were not increased. Certain CWs even describe retaliation by the company when they took measures to protect consumers from fraudsters or dangerous users.

5. The CWs also detail how these illegitimate and fraudulent accounts impacted and inflated not only Match's user statistics, metrics, and trends, but also its reported results, both directly, as a "significant" percentage of scam accounts paid for extended length (3-month, 6-month, or even 1-year) memberships, and indirectly, as Match and its branded websites and apps used "aggressive" marketing based on the illegitimate and fraudulent accounts to target legitimate non-paying users. Specifically, the CWs and an FTC complaint both assert that Match based email solicitations and other marketing on the illegitimate and fraudulent accounts that were designed to get non-paying users to upgrade to a premium or paid membership, like Tinder Gold, to see purported "winks" or messages from other accounts – that, in reality, were set up by non-existent "admirers" who sent only scam communications. The CWs said that Match and its branded websites and apps also made it confusing and difficult – by design – for users to cancel paid memberships once they were initiated.

6. Contrary to these negative, undisclosed facts, Defendants Match, Ginsberg, and Swidler made materially false and misleading misstatements and omissions to investors during the Class Period that depicted Match as a strong company with solid website / app user base, high customer satisfaction, and effective safety screening. For instance, in a December 20, 2018 video interview published by the *Wall Street Journal*, Defendant Ginsberg said, "[***W***]***e do everything we can to provide safety and security for our users – everything from one strike you're out to making sure that we put in processes and best practices across the organization to keep bad actors out***." A December 21, 2018 *Wall Street Journal* article published additional quotes by Defendant Ginsberg, including, "***It helps for us to have a portfolio [of matchmaking apps]***

because if there's bad behavior on one app, we can identify that user, we'll kick him off all the apps." In a February 7, 2019 CNBC video interview, Defendant Ginsberg said, "[***A***]***bout a year and a half ago, we introduced*** [***Tinder***] ***Gold, which*** … ***gives you the ability to see who's liked you***. [***I***]***f someone says to you, do you want to see all the women who've liked you or all the men who've liked you, it's very hard to say no***. … [***T***]***he take rate on that Gold or that 'likes you' feature was really high and that was priced at an even higher premium, another subscription tier***. … [***T***]***hat's what's really driven a lot of the growth***." In a May 8, 2019 *Yahoo! Finance* interview, Defendant Swidler said, "***We rolled out something called Tinder Gold about a year and a half ago now. It's been a huge success***. [***W***]***e're continuing to find ways to make that offering more compelling for users and have more people buy into Tinder Gold. We're merchandising it better. We're getting it in front of users more effectively. And it's really working***." Defendant Ginsberg wrote in an article in the July/August 2019 issue of the Harvard Business Review, "***Most dating apps, including Tinder, have shifted to a "freemium" or paywall strategy***. Joining is free, and users get basic functionality. ***They can opt to pay for premium features such as seeing who likes you and swiping in another city. Last year Tinder's revenue topped $800 million, demonstrating that many people are willing to pay for these features***." Match's September 25, 2019 press release, authorized for publication by Defendants Ginsberg and Swidler, stated, "***We catch and neutralize 85% of potentially improper accounts in the first four hours, typically before they are even active on the site, and 96% of improper accounts within a day***" and "***We've developed industry leading tools and AI that block 96% of bots and fake accounts from our site within a day and are relentless in our pursuit to rid our site of these malicious accounts.***"

7. The truth about these and the other alleged misstatements and omissions alleged below was revealed through a series of partial corrective disclosures that over time revealed, *inter alia*, that the FTC had filed a complaint against Match; that Match's legal costs were soaring; that an investigative report revealed that Match's websites and apps, including Tinder, failed to screen for sex offenders, leading to sexual assaults on legitimate site users; and that a Congressional investigation was launched into the legitimacy and legality of Match's user base. Each of these partial corrective disclosures was accompanied by a correlating stock drop, sometimes muted by Defendants' contemporaneous explanations and additional misstatements, and each of them damaged Plaintiffs and the Class Members. As a result of Defendants' wrongful acts and omissions as alleged herein, and the precipitous decline in the market value of Match's securities, Plaintiffs and the other Class members have suffered significant losses and damages.

II. JURISDICTION AND VENUE

8. The claims asserted herein arise under, and pursuant to, Sections 10(b) and 20(a) of the Exchange Act, 15 U.S.C. §§78j(b) and 78t(a), and SEC Rule 10b-5 promulgated thereunder, 17 C.F.R. §240.10b-5.

9. This Court has jurisdiction over the subject matter of this action under 28 U.S.C. §1331 and §27 of the Exchange Act.

10. Venue is proper in this Judicial District pursuant to §27 of the Exchange Act and 28 U.S.C. §1391(b). Many of the acts charged herein, including the dissemination of materially false and/or misleading information, occurred in substantial part in this District.

11. In connection with the acts, conduct and other wrongs alleged in this Complaint, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce,

including, but not limited to, the mails, interstate telephone communications, and the facilities of an electronic securities exchange in this District.

III. PARTIES

12. Plaintiff Phillip R. Crutchfield, as set forth in the previously-filed certification, incorporated by reference herein, purchased Match securities during the Class Period, and suffered damages as a result of the federal securities law violations and false and/or misleading statements and/or material omissions alleged herein.

13. Plaintiff Samir Ali Cherif Benouis, as set forth in the accompanying updated certification filed herewith and in his previously-filed certification, incorporated by reference herein, purchased Match securities during the Class Period, and suffered damages as a result of the federal securities law violations and false and/or misleading statements and/or material omissions alleged herein.

14. Defendant Match ("Match") is incorporated under the laws of Delaware with its principal executive offices located in Dallas, Texas. Match's common stock trades on the NASDAQ exchange under the symbol "MTCH." During the Class Period Match was a majority-owned, publicly traded subsidiary of IAC/InterActiveCorp ("IAC"). At relevant times, the Match corporate website has listed at least 20 different analysts who follow the company and its stock.

15. Defendant Amanda W. Ginsberg ("Ginsberg") was, at all relevant times, the Chief Executive Officer ("CEO") of Match.

16. Defendant Gary Swidler ("Swidler") was, at all relevant times, Chief Financial Officer ("CFO") of Match.

17. Defendants Ginsberg and Swidler are collectively referred to herein as the "Individual Defendants."

18. Defendants Ginsberg and Swidler, because of their positions with Match, possessed the power and authority to control the contents of Match's reports to the SEC, press releases and presentations to securities analysts, money and portfolio managers and institutional investors, *i.e.*, the market. Defendants Ginsberg and Swidler were provided with copies of Match's reports and press releases alleged herein to be misleading prior to, or shortly after, their issuance and had the ability and opportunity to prevent their issuance or cause them to be corrected. Because of their positions and access to material non-public information available to them, Defendants Ginsberg and Swidler knew that the adverse facts specified herein had not been disclosed to, and were being concealed from, the public, and that the positive representations that were being made were then materially false and/or misleading. Defendants Ginsberg and Swidler are liable for the false statements pleaded herein.

IV. NON-PARTY CONFIDENTIAL WITNESSES

19. Lead Plaintiffs' access to former employees of Match and its branded websites and apps to solicit statements of truthful, relevant information has been hampered by the existence of nondisclosure agreements and pending or potential personal litigation between these employees at the company. Lead Plaintiffs believe that subpoena discovery would yield additional, material information that would support the allegations and claims set forth herein.

20. CW1 worked as the Senior Manager of Financial Planning and Analysis for Match Group from January 2016 until May 2019 at Match Group's headquarters in Dallas, on the 13th floor where Defendant Ginsberg's office was located. In this position, among other things, CW1 reviewed financial reports from each of Match's website / app brands and consolidated them into reports for monthly forecast meetings attended by executive leadership, including Defendants Ginsberg and Swidler, worked on Match employee head-count reports, prepared information for

Match's then-parent company IAC, prepared information for quarterly investor calls, and attended monthly budget meetings. CW1 reported to Joaquin Martinez, the Vice President of Finance at Match Group, who reported to Indrajit Ponnambalam, the Senior Vice President of Finance who reported to Defendant Swidler. CW1 interacted closely with Defendant Swidler, whose office was located in Match's New York office, via approximately 2 video conference calls per week, in addition to monthly forecast meetings and quarterly investor calls. CW1 also had regular interactions with Defendant Ginsberg, meeting with her at least 2 times a month. CW1 interacted with Match's then-President and current CEO Sharmistha "Shar" Dubey during monthly forecast meetings, quarterly investor calls, or when CW1 had to put together a report for IAC.

21. CW2 worked as a Senior Finance Manager at Match.com in its Dallas headquarters from February 2016 to February 2019. In this position, among other things, CW2 analyzed Match.com's financial data, developed earnings forecasts, prepared financial data for weekly and monthly meetings where Defendants Ginsberg and Swidler were present, and worked with CW2's team to increase the conversion of non-paying members to paid member subscribers. CW2 reported to Senior Vice President Steve Bailey, who reported to Defendant Swidler.

22. CW3 worked at Match.com from May 2010 as the Director of Training and Quality Assurance in Match's Dallas headquarters, where CW3's work included developing training modules for employees, reviewing employees to see that they were meeting guidelines, and conducting customer service training for employees of Match.com and other Match brands. CW3 left the company in September 2019 when CW3's position was eliminated. CW3 reported to the Chief Operating Officer.

23. CW4 worked at Match.com from July 2014 until November 2017 as a Product Manager in the Operations Team at Match's Dallas headquarters, and then as a Senior Project

Manager in charge of web applications until July 2018. CW4 reported to Senior Vice President of Product, Beth Wilson. CW4 worked on various teams to improve Match.com's products, including photo recognition software and efforts to incorporate fraud detection on Match.com and back-end systems for customer service representatives to work with customers on billing and refunds.

24. CW5 worked at Match.com in its Dallas headquarters starting in October 2010 for a year as a customer service representative before moving into the Risk Operations Department (commonly referred to as the Fraud Department), where CW5 worked as a Senior Fraud Investigator until October 2019. Among other duties, CW5 investigated member profiles that had been flagged automatically by the internal fraud detection system and attempted to block accounts CW5 believed to be created by scammers. CW5 and the other Fraud Department members monitored profiles on Match.com and People Media Group, the group of sites owned by Match.com, that were internally referred to as Match's affinity brands and that included niche sites like ourtime.com and blackpeoplemeet.com. As a Senior Fraud Investigator, CW5 reported to the Fraud Department heads, Mike Hanson and Gary Snider.

25. CW6 worked at Match.com in its Dallas headquarters as a Senior Security Engineer from February 2018 until April 2019. Among other duties, CW6 was responsible for setting up security systems to detect security breaches, such as if a hacker was trying to access members' personal information. CW6 reported to the Director of Security for Match Group, Joey Mitchell. CW6 was one of six people on the Security Team.

26. CW7 worked as the Director of Finance for Tinder from July 2014 until December 2018 at Tinder's West Hollywood office. Among other things, CW7 conducted financial analysis

and prepared financial reports that detailed Tinder's key metrics and financials. CW7 reported to Senior Vice President James Kim.

27. CW8 worked at Match.com in Match's Dallas headquarters in a variety of capacities from 2011 through May 2019, most recently as the Manager of Community Operations/Relations (January 2018 through May 2019). In this position, among other duties, CW8 supervised the work of the third-party call center that served as the first line of contact for customers, which included a team of four escalation officers, a team of eight internal customer care agents, and a pilot program offering a "white glove" interactive approach for members who paid a premium price. CW8 reported to the Community Relations director, Crystal Roloff, who reported to the Vice President of Community Relations.

28. CW9 worked at Match.com in its Dallas headquarters from August 2018 until May 2019 as an Escalation Specialist, handling calls from customers who were not satisfied by the first line of customer service representatives. CW9 reported to the Escalations Manager, Amanda Harris. CW9 fielded calls regarding, among other things, subscribing customer complaints about Match.com's billing practices, about their inability to access "winks" (a way for members to indicate interest in someone else on the site that many members use to make first contact before sending a message) and messages on the site sent by other members sent to them before they chose to subscribe (so as to access those messages and "winks"), and about their paid subscriptions continuing even after they tried to cancel. CW9 was fired for receiving low scores from the Quality Assurance Department, in part, in retaliation for refunding customers' money and advising customers to hide their profiles when they told CW9 that they were afraid for their safety after interactions with other Match customers.

29. CW10 worked as a Senior Product Designer at Match.com in Match's Dallas headquarters from July 2018 until August 2019. Among other duties, CW10 worked on the desktop website design and mobile application design, making items on the site visibly appealing, reviewing metrics, and testing that the site's usability. CW10 reported to the Design Team Lead, Sean Lester. CW10 also suffered retaliation when CW10 was asked to leave, in part, because CW10 continuously questioned Match.com's methods, which CW10 said were all about metrics and not about the customer.

30. CW11 worked at Match's Tinder brand (as discussed below) at its corporate headquarters in Los Angeles from December 2017 to May 2018 in the Trust and Safety Division, as one of six Team Members whose duties included responding to user-generated reports about other users (such as if the users were sex offenders, or were involved in harassment or other inappropriate behavior) and then from May 2018 until April 2019 in the Customer Service Division, providing various tech support assistance. During CW11's tenure in the Trust and Safety Division, CW11 reported to Nicole Bloomfield, who reported to the VP of Global Community Operations, Victor Colomes, who in turn, reported directly to the Tinder CEO, Greg Blatt.

31. CW12 worked for Match.com at its Dallas headquarters from October 2018 until November 2019. CW12 was initially hired as part of a pilot program that was commissioned to help Match.com determine if its overseas call center addressed customers' needs and whether to continue to use it. In that position, CW12 responded to customer phone calls about their accounts. About halfway through CW12's tenure, the pilot program ended and CW12 was kept on as a Customer Experience Advocate. In this position, CW12 responded to customers' emails regarding problems with their accounts. CW12 reported to CW8.

32. CW13 worked as a Community Operations Manager at Tinder from August 2018 until June 2020, based in the West Hollywood office and reporting to Aaron Schlew. CW13 managed the team of Tinder employees who reviewed individual accounts flagged as potentially fake, fraudulent, or bad actors.

V. SUBSTANTIVE ALLEGATIONS

A. Match's Business & Operations

33. Match is a provider of subscription dating products servicing North America, Western Europe, Asia, and many other regions around the world through websites and applications that Match owns and operates. Match operates a portfolio of brands, including not only Match.com, but also other branded websites and apps that are purportedly designed to increase the likelihood of users in finding a dating connection. Match Group revenue is primarily derived directly from users in the form of recurring subscriptions. Subscribers pay in advance, primarily by credit card or through mobile app stores. Revenue is also earned from online advertising, the purchase of à la carte features and offline events. Many of its brands employ a so-called "freemium" model, which permits basic registration and functionality for free, but charges a paid premium for advanced access and features.

34. Match's portfolio of website / app brands is collectively available in 42 languages and offered in over 190 countries. Its key brands include:

- ***Match.com***. Match.com was launched in 1995. Match claims that among Match.com's distinguishing features are the ability to search profiles, receive algorithmic matches and attend live events, promoted by Match.com, with other subscribers. Match.com is a brand that purportedly focuses on users with a higher level of intent to enter into a relationship, with a product and marketing that are purportedly designed to reinforce that approach. Match.com relies heavily on word-of-mouth traffic, repeat usage, and paid marketing. Match.com generates revenue in ways that include users converting to paid memberships and through online advertising.

- ***Tinder***. Tinder was launched in 2012, and Match claims that it has since risen to scale and popularity faster than any other product in the online dating category with very limited marketing spend, growing to over three million subscribers. Tinder employs a freemium model, through which users can use many of the core features of Tinder for free, including limited swiping and communicating with other users. However, to access premium features, such as unlimited swiping, a Tinder user must subscribe to either Tinder Plus, launched in early 2015, or Tinder Gold, which was launched in late summer 2017;

- ***PlentyOfFish***. PlentyOfFish was launched in 2003 and acquired in October 2015. Match claims that similar to Match.com, among PlentyofFish's distinguishing features is the ability to both search profiles and receive algorithmic matches. Similar to Tinder, according to Match, PlentyOfFish has grown to popularity with very limited marketing spend and also relies on a freemium model, whereby users subscribe to a pay version to access premium features;

- ***Meetic***. Meetic, a European online dating brand based in France, was founded in 2001. According to Match, similar to Match.com, among Meetic's distinguishing features are the ability to search profiles, receive algorithmic matches, and attend live events promoted by Meetic with other subscribers and non-subscribers. Also, similar to Match.com, Meetic is a brand that focuses on users with a higher level of intent to enter a relationship;

- ***OkCupid.*** OkCupid was launched in 2004 and has attracted users through a mathematical and question-and-answer approach to the online-dating category. According to Match, OkCupid has grown in popularity similar to Tinder and PlentyOfFish without significant marketing spend and also relies on a freemium model, whereby users subscribe to a pay version to access premium features;

- ***OurTime.*** Match claims that OurTime is the largest of Match's affinity-oriented brands and the largest community of singles over age 50 of any dating product; and

- ***Pairs.*** Pairs was launched in 2012 and acquired in May 2015. According to Match, Pairs is a leading provider of dating products in Japan, with a strong presence in Taiwan and a growing presence in other select Asian countries. Match claims that Pairs is a Facebook-based dating app that was specifically designed to address social barriers generally associated with the use of dating products in Asian countries, particularly in Japan.

35. Match's brands enable users to establish a basic profile and to review other users' profiles without charge. Each website / app also offers additional features, some of which are free but some of which require payment. In general, access to premium features on Match-owned and -operated websites and apps requires a subscription, typically offered in packages ranging from

one to six months, with pricing differing within a given brand based on factors including the duration of subscription, the bundle of paid features a user chooses to access, and whether a subscriber takes advantage of any special offers. In addition to subscriptions, many of Match's websites and apps offer the user premium features, such as the ability to promote themselves for a given time period or to review certain profiles without any signaling to the other users, on a pay-per-use, or à la carte, basis. The precise mix of paid and premium features is established over time on a brand-by-brand basis.

36. Match's revenue is primarily derived directly from users in the form of recurring subscriptions, which typically provide unlimited access to a bundle of features for a specific time period, and the balance from à la carte features, where users pay a non-recurring fee for a specific action or event. Each of Match's websites and apps offers a combination of free and paid features targeted to its unique community, and thus, a key strategic goal of Match was to convert its free members into paid memberships and premium services. In addition to direct revenue from the users, Match generates indirect revenue from online advertising that makes up a much smaller percentage of its overall revenue.

37. Throughout the Class Period, Defendants Match, Ginsberg, and Swidler closely tracked many metrics regarding Match's websites / apps, including without limitation total registered members, number of members on a premium or paid membership (a/k/a the "paid member count" or "PMC"), the conversion rate from unpaid to paid memberships, and the average revenue per user (or "ARPU"), a figure that would diminish if Match spent more money to enhance security or safety features. Defendants Match, Ginsberg, and Swidler also tracked extensive "red flag" metrics, many in real time, including without limitation the raw numbers of scam or fraudulent member accounts, their percentage of total memberships, the rates at which they could

be removed, and unusual spikes in registrations or site activity that signaled mass-scale or "bot" attacks.

B. Match's Strong and Growing Revenues Were Driven By Widespread Undisclosed Misconduct

38. Contrary to Defendants' misstatements alleged herein and undisclosed to investors, as described by the CWs, Match's brands suffered from serious legitimacy issues regarding memberships, which affected its reported results. Specifically, certain of Match's brands, including Match.com, had rampant problems with widespread fraudulent accounts by scammers and so-called "bots" (autonomous programs that can interact with systems or users), which were illegitimate and designed solely to defraud *bona fide* members, while other brands, such as Tinder, failed to screen or to take sufficient steps to remove sex offenders and other dangerous users. Match and its brands advertised and marketed to legitimate users, seeking to have them switch to pay or premium memberships, based on messages, "winks," and similar communications generated by the illegitimate accounts. Match inflated its membership statistics and reported results by misleadingly driving up its paid subscriptions though these tactics and then making it difficult for users to end their paid service or to cancel their memberships. When Match's website / app brand employees sought to help customers, to protect them against dangerous or fraudulent accounts, or to get them a refund, they were retaliated against and rebuked by the company. The CWs, most of whom worked in the same corporate headquarters building as Defendants Ginsberg and Swidler and Match' senior executives and/or attended meetings with them during which the topics related to this lawsuit were discussed, demonstrate that Defendants Ginsberg and Swidler and Match's top leadership knew of or recklessly disregarded these material, undisclosed facts and financial risks to investors.

1. Undisclosed Facts and Risks Concerning Fraudulent Accountholders

a. Undisclosed Facts and Risks Due to Scammers

39. The CWs establish that Match's website / app brands were plagued by a huge volume of fraudulent accounts designed to defraud legitimate users and that Defendants Ginsberg and Swidler and Match's executive leadership knew of the problem but failed to sufficiently address it.

40. According to CW5, a Senior Fraud Investigator at Match.com, scammers' goal on Match's branded websites and apps was to get money or possessions from legitimate members. CW5 stated that, typically, scammers would pretend to be international businessmen or pretend there was a catastrophe of some kind, and then ask for money or gift cards. Knowing that Match.com's account activity and on-site messages were monitored, CW5 said that many scammers would try to get the real email addresses or phone numbers of members early so that scammers could more freely engage in fraud off the website or app. CW5 stated that the average lifespan of a scammer account was 15 hours, though some fraudsters were "slow burners," who would develop long-term communication with members before attempting to extort money. CW5, stated the majority of fraudulent users that plagued Match.com were from the Western coast of Africa, with CW4, a Senior Product Manager, specifying that scammer accounts specifically originated from Ghana.

41. According to CW3, the Director of Training and Quality Assurance at Match.com for nearly a decade, Match.com's fight against fraudulent accounts "was a widely known company struggle" during CW3's entire tenure. As CW3 put it, "romance scams and fraud accounts are not whisper words around Match." CW4 stated that Defendant Ginsberg was aware of Match's

struggles with fraudulent accounts and would speak up at company-wide meetings about fraudulent accounts.

42. Yet, Defendants Match, Ginsberg, and Swidler failed to implement sufficient countermeasures to remove fraudulent accounts or to ensure that those accounts did not harm legitimate members or adversely impact Match's reported metrics. Indeed, the CWs described an overworked, under-sized team of individuals engaged in a constantly evolving game of cat-and-mouse with huge numbers of fraudsters. CW4, a Senior Product Manager in charge of web apps, helped design backend programs for Match.com and understood the Fraud Department's processes. CW4 stated that the Fraud Department was constantly working to catch up with ever-changing tactics of fraud perpetrators. CW5 stated that certain factors would prompt an account to be flagged as potentially fraudulent, including: multiple failed payment attempts indicating possible use of stolen credit cards; a cloaked IP address or use of VPNs or other masking software that made it difficult for CW5's team to see the country of origin; sending more than the limit per day of messages, winks, or likes; reusing the same easily accessible photos from the internet; and the use of commonly misused American vernacular, both in messages and in profile language, typically from fraudulent accounts originated from Ghana, Nigeria, Russia, or Eastern Europe. CW3 and CW4 corroborated these factors. CW5 stated that any one of these factors, however, was not enough to set off the alert to check the account for fraud, but a combination of the factors would cause automatic flagging.

43. CW4 stated that only subscribing accounts were screened for fraud, on the rationale that non-subscribers did not have the ability to message other members. CW4 said that once an account was placed in the fraud queue, it was given a percentage score based on the likelihood of fraud, with scores above a certain threshold imposing certain messaging limitations, while lower-

scoring flagged accounts could be removed once a fraud inspector had the time to review the account.

44. Significantly, however, Match employed wholly insufficient resources to handle the rampant fraudulent accounts on its websites and apps. For instance, CW5 stated that the work in the Fraud Department was "never ending" and the Fraud Department worked around the clock, 24 hours a day, 7 days a week, 365 days a year, including all holidays during CW5's entire tenure at Match. CW5 stated that Fraud Department, comprised of just 8 members, were required to manually review a minimum of 1,200 accounts per day that were flagged by the internal fraud detection system and that they worked in shifts so that there was always someone working to manually assess accounts. CW3 and CW4 corroborated this assessment that accounts flagged as fraudulent had to be reviewed manually, with CW3 describing the Fraud Department as an overworked "24/7" team of workers manually reviewing automatically flagged accounts. CW3 stated that the Fraud Department at Match.com was constantly running to remove scammer accounts and that, as social media use grew, Match.com's fraud problems have grown as well. CW3 stated that "no matter how many accounts you pull down, it's a continuous fight – [fraudsters] just stick more right back up."

45. Because of the prevalence of fraudulent accounts on Match.com, some Customer Service representatives also reviewed accounts to determine if they were fraudulent. For instance, CW12 worked in the Customer Service Department responding to customers' concerns via phone and email, but was also responsible for detecting fraudulent accounts that had slipped through Match.com's automatic flagging process. Match.com subscribers would sometimes report suspicious activity from other members. When that happened, CW12 would pass on information about the suspicious account to the Fraud Department if it there were certain triggers, such as

improper use of English grammar. CW12 also deactivated or removed fraudulent accounts weekly. CW12 saw spikes in fraudulent accounts particularly during the Christmas holidays or the summer.

46. These measures failed to adequately address the problem, and as a result, a large percentage of accounts on Match.com were fraudulent. According to Finance Department analysis by CW2, Match.com's Senior Finance Manager at its Dallas headquarters, which was based on a comparison of the raw number of registrations on any given day against how many of those members were removed by the Fraud Department seven days later, 15% of all Match.com membership registrations were fraudulent. CW2 stated that the fraudulent registrations percentage remained close to 15% – an astounding one in six site members – at least throughout CW2's entire 3-year tenure. When informed that CW2 said that 15% of Match.com registrations were fraudulent, CW1 said that CW2 should be trusted to know that number because CW2, among other things, was involved in analyzing the Match.com figures, noting that CW2 spent about a week and a half every month preparing the detailed forecast report and looking at all of the financials for Match.com. Given the pervasive understaffing of anti-fraud efforts, these statistics meant an unattainably difficult task for Match's undersized Fraud Department. For instance, CW5 stated that, each day, CW5 removed about 30%-45% of the accounts CW5 reviewed on Match.com and its affinity brands because they were determined to be fraudulent. Indeed, CW5 stated that during CW5's more than 7-year tenure at Match.com, CW5 may have deleted about 1.7 million user accounts. CW5 added that CW5 was the third employee to break the one millionth blocked account mark at the time.

47. An even larger percentage of Tinder's accounts were fraudulent. According to CW7, Tinder worked with the assumption that approximately 20% of all accounts and other

account activity on the Tinder app were bots and/or fraudulent. Tinder's Director of Analytics, Bob Wilson, informed CW7 of this percentage first-hand. However, CW7 did not factor the percentage of fraudulent accounts into CW7's financial reports or analysis, in which membership numbers, including the PMC, were reported, but the raw numbers were not adjusted to remove the impacts of fraudulent accounts. CW7 stated, "whatever our subscription number was, we took that number at face value – we did not parcel it out when reporting membership numbers." CW7 said there was no doubt that there were fraudulent accountholders who paid to have premium Tinder account features, so as to further advance their fraudulent activities on the site.

48. Other CWs corroborated the statements by CW1, CW2, and CW7 as to the sheer numbers of fraudulent and bad actor accounts on Match branded sites and apps. For instance, when informed of their statements, CW11, who worked as one of six Trust & Safety Division members at Tinder before transferring to the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. Citing a nondisclosure agreement, CW13 stated that CW13 could not provide specific numbers to quantify, but said that Tinder definitely had an internal estimate of the amount of accounts on the site that were fake, fraudulent, or bad actors that the anti-fraud team had not caught, saying "There was knowledge of that." CW13 added that Tinder's estimates were tracked on an ongoing basis and were based on and fluctuated with the number of such accounts that were caught.

49. CW5, a Senior Fraud Investigator at Match.com who had a nearly 10-year tenure with the company, went even further, stating that of the up to 2,200 accounts flagged for potentially fraudulent activity that CW5 reviewed every day, CW5 blocked a low- to mid-40 percent for

engaging in fraudulent activity, and of those blocked accounts, a "significant" percentage were paid subscribers. CW5 gave an example of CW5 reviewing 2,000 accounts in a day and removing 800 of them for fraudulent activity, of which 400-500 would be paid subscribers. CW5 said that CW5's seven colleagues in the Fraud Department all had similar percentages. CW5 was confident that the company was tracking the percentage of fraudulent accounts that were paid versus unpaid.

50. CW5 explained that the reason such a significant portion of fraudsters paid for subscriptions was because they could not enact their fraudulent schemes without a paid membership, as only paying members can send messages to other users or read messages sent by other users. Any fraudster wanting to communicate with another user to extract money or conduct any other fraudulent scheme had to pay for a subscription or else he would lack a way to communicate with potential victims. As CW5 stated, fraudulent schemes, by their very nature, required fraudsters to pay for a membership, which is why such a significant portion of fraudulent accounts were paid subscriptions. CW5 said that although Match.com offered 1-month, 3-month, 6-month, and 1-year subscriptions and it might seem logical that fraudsters would pay the minimum amount for the 1-month subscription, in actuality, many fraudsters actually paid for the longer 3-month and 6-month subscriptions, likely in an effort to make the fraudulent account seem more legitimate, to "throw us off their trail," and to make it more costly for Match.com to remove the account and refund the account fees.

51. Defendants Match, Ginsberg, and Swidler were aware of fraud on Match's brands, but failed to take necessary actions to address it because of a preferred focus on the revenue-producing metrics of Match's branded websites and apps. In preparation for monthly forecast meetings, CW1, the Senior Manager of Financial Planning and Analysis at Match, would first meet with the financial department leaders of Match's brands who would provide CW1 with a deck

summarizing the brands' performance and forecasts, like the materials prepared by CW7 that did not adjust out the fraudulent accounts. At the direction of Defendants Ginsberg and Swidler, CW1 would then consolidate all the reports into a 30-minute presentation and report for the monthly forecast meeting, which was attended by Match executives including Defendants Ginsberg and Swidler, Match then-President and current CEO Shar Dubey, and CW1's two supervisors, Martinez and Ponnambalam. The monthly forecast reports contained financials that included various metrics, consolidated into a total and then divided by brand, including expenses, revenue, EBIDTA, the revenue compared to the prior year, the forecast, and the budget. CW1 stated more "granular, day-to-day" metrics, like the total number of users and the "net adds," which combined the number of renewal subscriptions and new subscribers in any given period, were provided as supplementary materials with the monthly forecast report.

52. Instead of accurately adjusting company forecasts to identify and then reduce fraudulent account activity, Defendants Ginsberg and Swidler were focused on revenue-generating metrics. For example, two key metrics in the monthly forecast reports were the number of paid members of each brand (the "PMC" or "paid member count") and the average revenue per user ("ARPU"), on which Match alternated focus based on external financial analysts' shifting emphasis. CW1 stated that Match would try to drive up PMC by offering heavily discounted, introductory pricing of 50% or more off monthly memberships, offering longer terms of memberships for the price of a shorter membership, and offering a more relaxed refund policy. According to CW2, the most intense push to increase PMC occurred at the close of a quarter or year end because Match wanted to meet its forecasts and appear as if its membership was steadily growing on earnings reports. CW2 stated that in the fourth quarter of 2018, there was a particularly intense effort for Match to meet it numbers because of a previous earnings call on which Greg

Blatt said that paid memberships would increase by the end of 2018. These PMC pushes would result in increased subscriptions, but there was an understanding, according to CW2, that many members who joined during the heavily discounted period would cancel their membership after rates increased. CW2 stated that this sometimes led to disastrous results for the following quarter because of the decline in paid members, such as occurred in the first quarter of 2019 – something CW2 had private conversations about with co-workers who expected the paid membership to immediately decline after the 4Q2018 PMC push. CW2 stated that another result of the discounts offered during the PMC pushes would be that by the next financial report, the ARPU would be lower. Then, Match would switch emphasis to increasing ARPU.

53. Focused far more on increasing Match's memberships and monetizing them rather than on ensuring that they were legitimate and posed no threat to *bona fide* users and by extension to Match's reputational capital, Defendants Swidler and Ginsberg were well aware of key metrics and tracked the numbers closely. CW1 stated that Swidler's focus was on topline growth of the PMC, explaining that Swidler wanted to first get the members in the door, and then find efficiencies within the company. According to CW2, Defendant Swidler was very involved in tracking PMC and would come to Match's Dallas headquarters approximately every six weeks to discuss how to increase PMC and what type of "gimmicks" they could employ to increase numbers to meet projections. Such methods usually included upselling packages and reducing rates. CW2, CW2's supervisor, Steve Bailey, and the Chief Product Officer at Match.com, Sushil Sharma, were among the attendees at these meetings. CW2 stated that when Swidler attended or called into monthly forecast meetings, CW2 would present the year-over-year numbers and they would discuss how to increase paid membership as well as how to set refund policies in order to maximize membership retention, as discussed *infra*. CW2 stated that Defendant Ginsberg was also present

during some of these discussions. CW2 stated that while Defendant Ginsberg was less involved in the Finance Department than Swidler, Ginsberg knew of efforts to boost up numbers prior to earnings reports and received daily reports on where the numbers stood. According to CW2 "everyone knew that we were chasing a number."

54. Defendants Ginsberg and Swidler knew that Match's brands had millions of fraudulent accounts infiltrating Match's branded websites and apps – indeed, CW5 was the third employee to surpass one million blocked accounts at Match.com alone – but they would only pay attention to the issue if it created a variance on the forecasted PMC or ARPU of the brands. For instance, CW1 said that the brand PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue became a constant topic during the monthly forecast meeting with Defendants Ginsberg and Swidler and Match executives. Because PlentyofFish had a smaller user base, removing fraudulent accounts had a bigger impact on its numbers in the financial reports. According to CW1, PlentyofFish's employees were constantly trying to weed out these bad accounts, but in doing so, PlentyofFish would revise its PMC/ARPU numbers downward as they were cleaning up the site. Month after month, PlentyofFish would consistently bring their forecasted PMC and ARPU numbers down, creating the impression that PlentyofFish was not putting enough effort to fix the problem of fraudulent accounts on its site. CW1 said that this created a point of frustration with Match executive leadership, particularly with Defendants Ginsberg and Swidler. CW1 clarified that Ginsberg and Swidler appeared frustrated that PlentyofFish kept reducing forecasts due to the removal of fake / fraudulent accounts and were "tired of hearing about it." CW1 added that due to Tinder's outsized impact on Match's revenues, Tinder received more resources for operations than smaller apps like PlentyofFish, which could

impact the amount of resources dedicated to identifying and removing fake, fraudulent, and bad actor accounts on the smaller platforms.

55. CW5 added that the Fraud Department was "not very well-liked" and a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back." CW5 explained that whenever the Fraud Department blocked and removed a fraudulent account, the Match.com system automatically refunded the entirety of the subscription fees, even in the case of longer 6-month or 1-year subscriptions, because scammers typically used stolen credit cards to pay for premium accounts. For this reason, CW5 said of the Fraud Department, "We were the most hated team." CW5 was confident that the company tracked the percentage of fraudulent accounts that were paid, because those involved significant amounts of refunds. As CW5 stated, "I do know for sure that Match as a company – they have those numbers. I know they do. The higher ups – they want to know that info. It was something that they always wanted to keep track of."

56. CW1 stated that Match's senior leadership would have known the statistics on the number of fraudulent accounts, specifically including Defendant Ginsberg and Match.com's CEO, Hosseini. CW1 stated that policies were decided upon by the board of directors, with Swidler, Ginsberg, and Dubey weighing in. According to CW1, policies would be the same across the brands and each brand would enact the policy with its own methods. CW1 was fairly certain this was how policy for fraud detection was set. Also, because Defendant Ginsberg also would have been aware of the numbers of fraudulent accounts due to having previously served as Match.com's CEO when Greg Blatt was CEO of Match. CW1 stated that Finance Department personnel who would have known about the specific fraud numbers at each brand included, CW2 and CW7. CW1 said that Defendants Ginsberg and Swidler also would have had more detailed discussions about

fraud with the Product Division or developers. Other CWs described the widespread knowledge of fraudulent accounts on Match websites and apps. For example, CW3 said "everyone in the building was aware of those issues. It was not a secret." CW4 also stated that everyone in the building had knowledge of the number of fraudulent accounts and that fighting fraud was a frequent topic at the twice weekly operations meetings.

57. CW5 added that an internal database at Match.com kept track of how many account profiles each Fraud Department investigator reviewed each day, how many were blocked for fraudulent activity, and a breakdown of blocked accounts into subcategories as to why the account was flagged, including reasons such as another user's email, the account's photo, or an internal algorithm system. CW5 could access the database, check it at any time, see the numbers for all Fraud Department investigators, and generate reports showing CW5's metrics or those of all the investigators in the Fraud Department.

58. Match's focus on metrics regarding the user base was evidenced and made available to everyone at headquarters via what CW6 described as a wall of screens in plain sight at the headquarters. CW6 stated that the security division was on the 14th floor of Match's headquarters, which was the main level that included the break rooms and conference rooms as well as the main entry for Match visitors. CW6 described the 14th floor as an open-concept area that included the Match.com's Operations Division, of which the Security Team was included. Within the Operations area, there were three or four large screen televisions mounted to a wall that had real-time site statistics. These statistics included general traffic patterns, server information, how many users were using the site at one time, CPU memory and information that indicated website health. CW6 stated that if there was an unusual traffic spike, it could indicate to CW6 that it was due to "bots" or because fraudsters had found a new way to avoid detection on the site. CW6 was aware

that Match.com's business was cyclical, with membership peaking at different points during the year, because Match.com posted this information on the wall of screens. CW6 stated that many people at the office would have been able to see this wall of screens with information about users if they were on the main floor of the company's offices or visiting the break room given the open-concept design of the main floor.

59. Other CWs who worked in the Dallas headquarters, which only had three floors, also said the wall of screens were highly visible. For instance, CW1 stated that the wall of screens displaying website statistics behind one of the social areas on the 14th floor and that that CW1 would see them when going to the big cafeteria, social areas, and conference rooms. CW1 stated that the wall of screens was in plain view and that if you know what you are looking at, then you could decipher them. CW9 corroborated that the wall of screens was highly visible.

60. Yet, despite the large percentage of fraudulent accounts on the Match sites, and despite the widespread knowledge of the prevalence of those accounts and the difficulties removing them, Match refused to increase fraud detection staffing to properly address the problem. CW1 stated that each brand would have their own systems and staff to combat fraudulent accounts. For instance, a group of just 8 people were tasked with reviewing flagged accounts on Match.com and its affinity brands. CW5 stated that there was implied pressure within the Fraud Department to keep up the review pace and that CW5 would spend just 5 to 15 seconds per profile to analyze whether it was fraudulent. CW5 would spend only a minute or more on flagged accounts that were not as obvious to resolve. CW5 stated that there were times that it felt that it was easier to let some flagged profiles retain an account rather than remove a profile erroneously. According to CW5, the Fraud Department would have benefitted from additional workers. However, when CW5 and others in the Fraud Department asked their supervisors for additional help, they were told that a

purportedly forthcoming, new, tougher registration system, that included text message verification, would alleviate their workload. Yet, by the time CW5 left Match.com in October 2019, this promised system to enhance security measures was not in place. CW5 stated that it was a "no-brainer" to have such a system noting, "if you make it harder to sign up, you keep away the riff-raff. I don't know why something wasn't implemented sooner."

61. However, the prioritization of profit over security by Defendants Ginsberg and Swidler made it a foregone conclusion that Match.com did not get the resources it needed to properly combat fraud, given that Tinder was Match's most lucrative brand. According to CW1, Tinder was "growing like a weed" and on a "rocket ship trajectory" of growth. Match.com and older brands that were not seeing rapid growth or revenue were operating with half the number of staff dedicated to fraud. CW1 said that Match.com was more or less just breaking even on its paid membership count and was just treading water like all other brands other than Tinder. CW2 stated that there was an attitude of acceptance within the Finance Department at Match.com that fraudulent accounts were on the site and it was regarded as routine and "business as usual." CW2 stated that Match.com did not ignore the fact that there were fraudulent users, but it was not viewed as urgent if fraud remained steady and did not suddenly spike. So, too, was the attitude at Match Group. As CW1 put it, Match's primary focus was on Tinder and its growth. Fraud was accepted on the websites and apps as long as there was no adverse variance in the brands' key metrics.

b. Undisclosed Facts and Risks Due to Bots

62. "Bots," or internet robots, can be utilized to perform automated repetitive jobs or they can be malware used to gain total control over a computer. Such bots are present on Match websites and apps. CW6, Senior Security Engineer at Match.com, stated that among the activity bots would perform on the Match.com site included harmful actions such as creating fraudulent

accounts and breaking into other user accounts. CW5 stated that the Fraud Team would often alert the Development Team, which included programmers and was largely responsible for identifying and shutting down bots, of unusual patterns that could be caused by bots. One of CW6's main job functions was to detect the presence of bots on Match.com and to try to install preventative measures to prevent their infiltration. CW6 stated that advanced bots would be able to fly under the radar and it would take a lot of human effort to detect the problem areas. As CW6 stated, occasionally, if the bot was not advanced, a script might be run that caused a specific request to be run a thousand times and it was immediately obvious based on the activity posted on the server screen the Security Team monitored that there was an active bot on the site doing something such as guessing passwords.

63. Defendants Match, Ginsberg, and Swidler failed to implement sufficient proactive or countermeasures to remove bots from Match's websites and apps or to ensure that those bots did not harm legitimate members or adversely impact Match's reported metrics. As CW6 described it, Match.com was often on the defensive working to prevent attacks by hackers and those who create malware. According to CW6, every time they would find a group of bots, the bots would change their approach so that preventing bots from infiltrating the Match.com website was a constant fight. For instance, CW6 said that if the bot activity was aggressive enough, it would show up on the monitoring screen and the Security Team would often find that those controlling the bots slowed the activity down to reduce the risk of detection. CW6 stated that they were just trying to keep up with new threats – the bots were the ones coming up with the rules of the game.

64. Defendants Ginsberg and Swidler were aware that bots were infiltrating the Match brands' websites and apps and causing harm to legitimate users by creating fraudulent accounts,

among other things. As CW6 stated, any website that gathers personal information is subject to such threats. Moreover, the wall of screens describe by multiple CWs at Match's headquarters could reveal "bot" activity in real time, in plain sight. Thus, the Match brands were aware that the websites and apps were prime candidates for unwelcome visitors.

c. Undisclosed Facts and Risks Due to Sex Offenders and Felons

Despite screening, there are sex offenders on Match.com

65. In the wake of a lawsuit against Match.com by a woman in 2011 who said she was sexually assaulted by someone she met through the website, Match.com implemented a system to screen memberships for sex offenders against a national sex offenders registry. However, this system has inherent limitations – users who registered with a credit card could be searched while users who registered via app stores and in-app purchases could not be searched, because the app stores controlled the registration data that Match.com needed to run searches. Even where users registered directly with Match.com, it lacked the precise data set (full name, birth date, accurate mailing address, etc.) needed to run a sex offender registry search – in part because Match.com intentionally did not seek it, over concerns about privacy or intrusiveness. Among the subset of registered users that could actually be searched despite all these limitations, Match.com flagged 3% of all users as having a hit on sex offender registries, at which point manual review of photographs was undertaken.

66. CW8, the Manager of Community Operations (a/k/a Customer Care and Community Relations) at Match's Dallas headquarters, personally worked to screen the site's memberships for sex offenders. CW8 stated that CW8 was one of up to four people who had access to the queue of profiles needing review and together they were expected to work through the queue. CW8 stated that Match.com's backend system checked subscribing member's billing

names against the national sex offender registry. CW8 explained that if a name matched with a name on the registry, CW8 or one of the others with access to the queue would check the person's profile picture against the photo publicly available on the registry. CW8 stated that they would look for other factors that matched, such as the race, hair color, and age, to verify it was the same person. CW3 and CW9 corroborated this process. CW3 said that there was some photo screening software that checked against photos of registered sex offenders and would flag individuals. Then, someone at Match.com would review flagged profiles to see if they were the same person. CW9 also stated that there was just one person at Match.com, James McMillan, who had a reactive role in investigating serious customer concerns, including complaints of registered sex offenders on the site. There were other measures taken to screen for sex offenders on Match.com. CW3 stated that Match.com would catch sex offenders as they were doing audits. CW8 said that there was an eight-person team separate from the Fraud Team that looked into complaints about members from members. If someone was reported to be a sex offender by another Match.com member, CW8 said that the team usually took the person's word for it and removed the profile.

67. However, there were still sex offenders Match.com. CW9 stated that Match.com did not employ any method to prevent sex offenders from signing up on Match.com in the first place. CW8 stated that there was probably one person a day removed from Match.com for being a sex offender.

Match.com allows felons to operate on the site unabated

68. Additionally, there were felons on Match.com. CW10, a Senior Product Designer at Match.com in Match's Dallas headquarters from July 2018 until August 2019, stated that Match.com did not screen for felons. CW10 said whether to screen for violent felons was a big

subject of conversation in the workplace. According to CW10, "you could be going on a date with a murderer and not know it."

Tinder does not screen for sex offenders at all

69. Given Match.com's half-measures to screen for sex offenders, the total lack of any such measures on Tinder, Match's most profitable website / app brand, is particularly egregious. CW11 worked at Tinder at its corporate headquarters in Los Angeles from December 2017 to May 2018 in the Trust and Safety Division, as one of six Team Members, responding to user-generated reports about other users, and from May 2018 until April 2019 in the Customer Service Division, providing tech support. During CW11's tenure at Tinder, CW11 stated that there was no proactive screening for sex offenders whatsoever. According to CW11, any sex offenders removed from the Tinder app were only found after other users proactively reported them to the Trust and Safety Division. In other words, Tinder let its users be put at risk and then left it to them to report what happened, possibly after a sexual assault or other threatening situation, before the company took any action. CW11 would see a sex offender complaint once every few weeks.

70. Moreover, the process for Tinder users to report sex offenders and other inappropriate accounts was not straightforward or efficient. CW11 stated that user-generated reports were generated within the Tinder app or via email and that there was no phone number available to make a report. Within the mobile app, CW11 stated that a user could elect to report another user by clicking on that person's profile and selecting an ellipsis symbol on the page that would prompt a drop-down menu that included one option, "report user." CW11 stated that if someone tried to report a user, the app would give the user categories for reporting the person, such as harassment. However, according to CW11, there was not a category for sex offenders and that if a person wanted to report a sex offender, there as an option to select "other" and the person

could write in sex offender in the category. CW11 stated that if a user reported someone as a sex offender, these key words would trigger the alert to go up higher in Tinder's system so that a Trust and Safety Team Member could address it quickly. CW11 stated that once the Trust and Safety Team received a sex offender report, the Team would first take the information provided by the complaining user and try to verify if the reported person was on the sex offender registry. If the report was verified, then it was an offense that could lead to the person being banned, according to CW11.

71. Despite knowing of sex offenders on the site, Tinder did nothing to prevent more from signing up in the first place. CW11 was also not aware of any methods in place to pre-screen sex offenders for signing up on the Tinder site in the first place. CW11 stated that inquiring whether a person was a sex offender was not a direct question asked to members when they signed up for an account. Moreover, according to CW11, Tinder's process for creating a user profile included filling out a short, simple form that would prompt an email to be sent to the user's given email address to accept the Tinder's terms and conditions. CW11 stated that once the terms and conditions were accepted, the person could start using Tinder. According to CW11, the goal of Tinder was to make signing up as easy as possible – "you don't even have to put your real name down."

72. Defendants Ginsberg and Swidler were aware that there were sex offenders and other bad actors on Tinder. According to CW1, Dubey, Match's then-President and current CEO, was very hands-on and in the weeds with Tinder's operations during CW1's tenure at Match. CW1 specifically recalled a period of about six months in 2017, after Sean Rad (Tinder's founder) left Tinder, that Dubey dramatically increased her time spent at Tinder's office to three to four days a week and started calling in from Tinder's Lost Angeles office for meetings that were occurring at

Match's Dallas headquarters and that she had previously attended in person. CW1 stated that Dubey's presence at Tinder continued until Match Group brought in Elie Seidman, who had been running OKCupid, to run Tinder. CW1 stated that if there were any red flags with Tinder's operations, Dubey would have been aware of them. Due to Dubey working so closely with Defendants Ginsberg and Swidler and other executive leadership, CW1 stated they too would have been aware of any red flags at Tinder, including policies not to screen for sex offenders and bad actors on Tinder's site. During the time that Dubey was at Tinder's headquarters, she would interact with Ginsberg daily and with Swidler several times per week, CW1 said. CW1 had first-hand knowledge of these facts and circumstances, because CW1 regularly had conversations with Dubey prior to the start of telephonic meetings in which they both participated.

73. For Defendants Ginsberg and Swidler and Tinder executives, preventing fraudulent accounts or accounts that posed risks to other members, such as those created by sex offenders, was not a priority as long as fraud or misconduct on Match's branded websites and apps did not cause a variance in the PMC or ARPU metrics. CW1 stated that as the most profitable of all the Match brands because of its rapid growth and usage, Tinder had the most resources available to identify and remove fraudulent accounts. However, according to CW1, most of the discussions about Tinder were related to its growth and not about combatting fraud and removing sex offenders from its site. CW1 stated that Defendant Swidler's comments about Tinder were usually centered around its growth and positive results, saying things like, "everything is going great – keep bringing me awesome numbers."

2. Undisclosed Facts and Risks Concerning Match's Use of Communications from Fraudulent Accounts to Generate Deceptive Marketing, Sell Subscriptions, And Increase Its User Base

74. Match.com's advertising and marketing emails to members varied greatly depending on whether members were subscribers (*i.e.*, paying members) or non-subscribers (*i.e.*, non-paying members) that Match.com was trying to entice into a paid membership by reference to purported communications by other site users. CW2 stated that marketing emails from Match.com to non-subscribers were "annoying" and "aggressive," and Match.com "would promote all messages, even if they were fraudulent." CW2 stated Match.com tried to engage new users and get them to send messages. CW2 conducted an analysis on what actions made non-subscribers decide to pay for a membership. CW2 stated it was "definitely over 30%" of members who subscribed after receiving a notification that they had a message they could not read unless they paid for membership. This percentage was higher for men who received messages from women and then immediately subscribed to read the messages. CW2 stated that a percentage of the messages marketed to non-subscribers were fraudulent. CW3, who was familiar with the incidence of non-subscribing Match.com members receiving emails notifying them that other members had liked them or sent them messages, stated that non-subscribing members receive emails on all their account activity, with the goal of getting them interested in paying for a membership to the site. Subscribers, on the other hand, do not get emails on every activity. CW2 stated that CW10 said that the automatic messages sent by Match were reworked about once a year through a contracted third-party firm that brought in temporary employees to work on the notification systems in Match's Los Angeles office.

75. After non-subscribers are induced by Match's emails and advertisements to pay for subscriptions, many of these new subscribers discovered that the people who "liked" them do not

exist in reality. CW3 stated that a frequent complaint CW3 received from subscribers was that they received an email stating that people liked them, but by the time they signed up and went to search for those people, they saw that those accounts were either not real or had been removed. CW10 was also aware of emails telling customers they had messages waiting for them, but the messages were not there once customers subscribed and searched for them. This was confusing for a lot of people, particularly if it happened multiple times a week, because it led the newly induced paid members to feel that they paid for a subscription but were not really getting the traffic they expected. CW8, who had been at Match.com in various roles in the Customer Relations Division since 2011, but most recently, worked as the Manager of Community Operations (a/k/a Customer Care and Community Relations) at Match's headquarters, stated that customers complained that they would sign up for a subscription and then be unable to see messages that were advertised as waiting for them. CW8 stated that CW8 was directed from the product department, possibly from the VP of Product, to tell customers that the account that sent the message was removed from the site. CW8 stated that CW8 and other customer care representatives had to be voice of the company and that "agents just say what they are told to."

76. Consumers were often unaware that, in many instances, communications received from Match.com are not from users interested in establishing dating relationships, but are instead from persons seeking to perpetrate scams. CW4 also stated that non-subscribers would receive emails and notifications from Match.com that they had a message waiting for them, sign up for an account, and then the message was no longer there. CW4 attributed the account disappearance to a flagged account scoring low enough that the account was still flagged and pending review, but not high enough to be automatically deleted. As CW6 put it, flagged accounts had to meet a certain threshold that were detected by Match.com's systems according to a complex algorithm developed

by internal engineers. CW4 stated that this threshold was high. CW3 stated that since nonsubscribers were emailed about all account activity, emails from Match.com would reach nonsubscribers about account activity from flagged accounts before they were removed. CW2 corroborated, stating that if a "bot" or suspicious fraudulent account liked the profile of an unpaid member, the message from Match.com notifying them of that activity was instantaneous.

77. It was widely known within Match.com that its subscription model was to get as many people to subscribe as possible and to hope that the subscribers forget that they subscribed and continue to pay through the automatically renewed subscriptions. CW1 stated that it was an "open secret" at Match.com that it relied on members subscribing for its service and then forgetting they had had signed up. CW2 corroborated this statement. CW1 would say in jest to co-workers things like, "who knows how many months this person has been married and forgotten that they are paying for Match.com because they don't follow their spending?" CW10 corroborated this stating "we had a lot of conversations – it was a daily task on how to figure out how to get people to sign up and forget about it." According the CW1, Defendant Ginsberg, who focused on the Match.com site, knew about this tactic and would have been keenly aware of this method.

3. Undisclosed Facts and Risks Concerning Match's Use of Deceptive Guarantees and Confusing Billing and Cancellation Practices to Maintain Its Improperly Inflated User Base

78. Once Match induced customers into signing up for paid subscriptions based on marketing fraudulent profiles, Match used deceptive guarantees and convoluted billing practices to prevent customers from easily cancelling their accounts.

a. Undisclosed Facts and Risks Concerning Match's Use of Deceptive Guarantees

79. CW3 stated that some consumers who visited Match.com were offered a match guarantee if they purchased a six-month subscription – whereby if they purchased a six-month paid subscription but did not meet someone special during the first six months, they would get an extra six months free. What was not explicitly stated on the website's offer notice, but the difficulty most people had, according to CW3, was that they had to certify that they met certain requirements before they could receive the six months of free membership.

80. CW9, an Escalation Specialist at Match at its Dallas headquarters, stated that there were four guidelines to qualify for the six-month guarantee, which included messaging at least five different people each month, having an active profile photo at all times, and having the profile public at all times. CW3 corroborated that the guarantee requirement included that subscribers had to contact five different people every month, but some people did not realize it was required to receive the free six months. CW9 stated that those terms were not up-front and were not advertised when a member sighed up for the six-month membership with the guarantee. Instead, members had to go to a separate page on the website to find those terms. CW9 stated that the terms page was found via a drop-down menu on the top right side of the page that said, "Match Guarantee." Additionally, CW9 stated that the terms were stringent. For example, in addition to having to message at least five people a month, CW9 said that if customers hide their profiles for a day or even for a couple of minutes, then they failed to qualify for the guarantee. Before the promotion was discontinued, CW9 stated that CW9 got to a point in escalation meetings where CW9 asked to give refunds or membership extensions. According to CW9, "it was getting so ridiculous." CW9 would say in the meetings, "we have to make some exceptions for this – people are calling every single day."

b. Undisclosed Facts and Risks Concerning Match's Improper Billing and Cancellation Practices

81. CW9 stated that the majority of customers CW9 spoke to had problems with billing. CW8 corroborated this statement saying that as the manager of community relations, Match.com received about 2,000 phone calls a day to their outsourced phone center, 1,000 emails a day and possibly as many as 500 chats via the website per day. According to CW8, there was always work to do, always more calls to take and more emails to answer. CW8 stated that overtime was sometimes mandatory with some people on CW8's team of approximately eight people working four hours of overtime a day. CW12, a member of CW8's team, had a quota to respond to 16 emails every hour, which CW12 stated provided little time to adequately devote to each customer issue. CW8 stated that CW8's department did not receive funding to hire additional people and they were a lower status department within the company because it was not revenue-generating. CW3 stated that fake profiles were the most common customer complaint and billing complaints were second most common.

82. As several CWs attest, it was well-known at Match.com that its membership cancellation policies were purposefully convoluted and harsh to discourage paid members from unsubscribing. For instance, CW2 stated that Match.com's membership cancellation policies were unnecessarily stringent and not up to industry standards. CW2 stated that membership cancellation was purposefully hard to locate and complete on the website and that it was part of Match.com's process to make sure cancellation was hidden. CW9 stated that Match.com was unethical in trying to prevent membership cancellations. CW9 stated that cancelling membership was a cumbersome process, with customers having to click through between five and seven screens. CW8 corroborated, stating that the cancellation process confused customers and that most customers who called Match.com complained that they had cancelled their membership but were still getting

billed. Like CW9, CW8 stated that the cancellation process required members to click through seven screens. CW8 stated that on one of the final screens, there was a survey asking members why they were cancelling. CW8 stated that most members thought they concluded the cancellation process before reaching the survey, but in actuality, by design, it was necessary to click "next" to confirm the cancellation again. Failing to complete the entire lengthy cancellation process resulted in customers unknowingly continuing to be billed, according to CW8. CW10 corroborated that the cumbersome cancellation process required people to go through several screens and that the button to request a cancellation was put in a hard-to-find spot. CW10 stated that Match.com "blatantly hid the cancel subscription button." According to CW10, the process to cancel was "ridiculous." CW2 stated that it was easier for members to cancel their subscriptions through the Apple or Android systems because there were fewer screens to click through. For this reason, marketing emails from Match.com included links that would direct non-paying users to the website and not the app, while subscribers were directed to the app.

83. CW2 stated that the cancellation policies would become even more stringent around quarterly and year-end reports, when the company wanted to show more paid members. During this time, Match.com would clamp down on membership refunds for any reason. CW2 said that Match was focused on hitting numbers, meeting estimates, and doing what it could to "prop things up." CW2 stated, "we would say we were trying to create brand value, but then at the end of every quarter, we'd discount 50 percent and we would hammer down on our refund policy – those were our two levers."

84. CW6 stated that Match.com's internal backend system logged everything a user did and created a record of all activity on the site. For example, according to CW6, a customer sales representative could tell if a user had tried to cancel but not been successful at submitting the

cancellation and had not been continuing to access the site. CW6 also said that when a user tried to register, that activity would be logged based on the user's IP address so that IT staff could tell when and where a user tried to access the site. Thus Customer Sales representatives at Match could therefore verify if users tried to cancel in earnest and, in theory, offer refunds or honor *bona fide* cancellation requests. However, Match.com's company-wide policies, based on efforts to increase and maintain its user base, stood in the way of Customer Service representatives freely honoring refund and cancellation requests.

85. Many customers also inadvertently renewed their membership after they successfully cancelled it. CW9 stated that after members cancelled their membership, they would still have time left on their membership before they could no longer access the paid features. According to CW4, if users cancelled their accounts but had unfinished time left on their contract, then they would have still been billed for the remainder of their contract. CW9 stated that it was very easy for customers to accidentally reactivate their membership during that period, because there was a button on a member's page that if clicked, would reactivate the membership. According to CW9, this triggering button was promoted in emails to members who were approaching their cancellations, and it was not clear to members that they were reactivating their membership and effectively reversing the cancellation. CW9 stated, "it blew my mind - I thought, this is not ethical." CW10 corroborated CW9's statements about the triggering button, saying that the reactivation button was simple to use and would not tell members that they would be charged for a full year if it was clicked.

86. Significantly, members who requested refunds due to encounters with fraudulent accounts were denied refunds. For instance, CW2 stated that refunds were based solely on how much a member used the site. So, if a member used Match.com, but found that most of the people

they interacted with were scammers or bad actors, they would not be given a refund. According to CW2, requests for refunds for this reason were viewed as simply not liking the product, which is not a basis for receiving a refund if members used the product. In addition, according to CW9, Match.com refused to refund customers who subscribed based solely on emails and marketing ads they received from Match.com alerting them to winks or emails from potential suitors whose accounts were subsequently removed.

87. Match clearly prioritized inflating its membership statistics over ensuring the legitimacy of its membership base and the safety of its site users. Even in instances where customers were afraid for their safety based on interactions with other users, CW9 was directed to avoid offering refunds and to not suggest or encourage hiding their profiles as an alternative. CW9 stated that a customer who met someone through Match.com learned that the person had been convicted for kidnapping. The customer was afraid for her children and CW9 sympathetically advised the customer to hide her profile on the site. As a result of that suggestion, CW9 received a failing score on an evaluation by Quality Assurance for that call because CW9 was not supposed to advise members to hide their profiles. In response to the failing score, CW9 stated that she wondered of CW9's supervisors, "Are you not even a human being?" CW9 stated that CW9 was told not to mention to members that they could hide their profiles or encourage them to do so because the company wanted as many users as possible featured on their site.

88. The lack of safety concern by Match's highest-level executives extended to its employees as well. CW1 said that at least a half-dozen times, Match Group received some periodic threat or complaint that prompted the company to bring in armed security guards stationed at its headquarters entrances for a week. CW1 said that CW1 only knew that some kind of threat prompted the enhanced security, but did not know whether it was an angry caller making

unspecified threats or a detailed threat against the company. According to CW1, when the armed guards were present, there was "no communication whatsoever" about the nature of the threat to employees, nor were there any communications thereafter as to policy changes, if any, made in response.

89. CW9 stated that beyond the cumbersome cancellation process, CW9 spoke with members who were misled about how much their recurring membership would cost. For example, CW9 said that members who signed up for a membership after receiving a promotional email about messages waiting for them to read would be offered a "sign up today and pay $25 a month" offer. However, according to CW9, that promotional value was only offered for the first month of renewal and the following months reverted to the regular rate of $40 a month. CW9 stated that other customers did not understand that the membership was a recurring billing - that information was in the fine print. CW10 described a similar deceptive process designed to keep users locked into subscriptions, saying that one issue of constant redesign was the rate card, which showed prospective members various subscription options and their costs. CW10 reworked the design of the card hundreds of times. CW10 stated that those options, which included a one-month membership and various bundles of months, did not spell out that the multi-month memberships were paid all at once. CW10 did, however, design many versions that specified the amount for the six-month membership, which was approximately $129, but CW10 stated that those designs were always rejected by superiors who were in charge of the product. According to CW10, "We were always trying to deceive with the messaging. It was not about the customer. It was all about metrics." CW10 stated that, generally, if there were terms and conditions for an offer, Match would hide them.

90. CW6 stated that customers complained about difficulty cancelling their accounts and that internally, Match realized it was an issue. CW6 stated that CW6's knowledge of customer complaints regarding difficulty cancelling accounts and Match's efforts to address the issue came from a company-wide meeting held just after CW6 joined Match in 2018. CW10 stated that in recurrent meetings (occurring around every three months) with senior leadership, including Match.com CEO Hesam Hosseini, Vice President of Product Dushyant Saraph, Product Manager Brett Richards, and Supervisor Sean Lester, CW10 discussed where to place the membership cancellation button so that users would be able to find it. CW10 recalled saying at a meeting, "My mom is a single mom. She's an older user. She got confused. Let's make this easy for the users." CW10 stated these meetings were hostile, that the cancellation process was a "touchy subject" for those in the Product Department, and debates about placement of the button to request a cancellation remained ongoing as of CW10's departure in August 2019.

91. Defendants Ginsberg and Swidler were aware of customer complaints and trends in customer issues. Both CW2 and CW1 stated that Defendant Ginsberg projected herself internally as being very much about product, brand messaging, and public relations, and so would have company-wide discussions about user experience. Therefore, Defendant Ginsberg would have known about consistent complaints that Match.com subscriptions were difficult to cancel. There were also reports available to Defendants Ginsberg and Swidler regarding customer complaint. For instance, CW3 stated that any major issue would trigger an internal report and that customer complaints were put into such reports. Also, according to CW8, there were daily breakdowns produced about the number of complaints received from customers. CW8 stated that each customer phone call would prompt the creation of a ticket and that there was an internal system to run a query on tickets. In addition, CW3 stated that customers would contact the CEO,

CFO, and other company leadership directly by going on to the company websites, figuring out the naming convention for company emails (*e.g.*, first initial plus last name at the company email extension) and send their concerns directly to them.

92. Despite knowledge about fraudulent accounts and the variety and multitude of customer complaints, Defendants Ginsberg and Swidler intentionally turned a blind eye and focused instead on Match's bottom line – which according to CW9 was to increase its user base and then to maintain that user base at all costs. According to CW9, Match did not care about its users finding relationships, but solely cared about growing its user base. CW10 corroborated this statement stating that the business was metrics-driven – it was never about the user.

4. Undisclosed Facts and Risks Concerning Match's Retaliation Against Its Employees Who Tried To Protect Members

93. Match retaliated against employees who did not support its bottom-line focus of growing and maintaining its paying user base at all costs.

94. According to CW9, Quality Assurance calls were based on whether Escalation Team members followed the script, avoided offering refunds, and did not mention membership cancellation. If the customer requested cancellation, CW9 stated that CW9 was supposed to try to talk them out of it. As discussed *supra,* CW9 received a failing score on an evaluation by Quality Assurance for advising a Match.com customer, who feared for her own safety and that of her children after being matched with a convicted kidnapper, to hide her profile. CW9 was told not to advise members that they could hide their profiles or encourage them to do so, because the company wanted as many users as possible featured on their site. CW9 also gave refunds to members who said that they misunderstood how much recurring membership would cost unless they did something (like use the membership for an entire month) and then requested a refund after the fact, drawing further company rebuke. CW9 stated that CW9 was fired for receiving low

scores on calls, due to CW9's refunding customers' money and allowing customers afraid for their safety to hide their profiles.

95. Similarly, CW10 had questioned Match.com's methods and refund policies due to concerns that they were not geared towards users and due to being upset that Match.com would not give a refund to CW10's own mother, who had trouble cancelling her membership. CW10 said that CW10 was asked to leave the company after disputes over these issues with CW10's supervisor.

C. Materially False and Misleading Statements Issued During the Period

96. During the Class Period, Defendants made materially false and misleading statements that can be organized into two primary threads of the alleged fraud: (i) the Membership Integrity Fraud and (ii) the Reported Results Fraud. Defendants' false and misleading statements, the reasons why each was false, and the categories of their fraud are described below.

1. The Membership Integrity Fraud

97. Defendants made a series of public statements and filings regarding the integrity and quality of the membership that were materially false and misleading.

98. On November 6, 2018, the company issued a press release (the "11/6/2018 Press Release"), which was filed with the SEC on November 6, 2018 as Exhibit 99.1 to Form 8-K signed by Defendant Swidler (the "11/6/2018 Form 8-K"), announcing its financial results for Q3 2018. It stated as "Q3 2018 Highlights" that **"*Total Revenue grew 29% over the prior year quarter to $444 million, driven by 23% Average Subscriber growth and 6% ARPU growth***" and "***Average Subscribers increased to 8.1 million, a 23% increase over the prior year quarter***."

99. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People

Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by

a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8

people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

100. On November 7, 2018, Match held a conference call to discuss its Q3 2018 financial results (the "11/7/2018 Investor Call"), during which Defendants Ginsberg and Swidler both spoke.

(a) During the 11/7/2018 Investor Call, Defendant Ginsberg stated the following in prepared remarks:

- ***Tinder remains the center piece of our growth story***. Direct revenue at Tinder was up nearly 100% in the third quarter compared to last year and subscribers grew 61% and ARPU rose 24%.

- In early Q3, we started testing Picks, which is an incremental feature that we introduced as part of the Gold package to enhance our subscription. ***Picks provide Gold Subscribers with a personalized daily list of interesting users***. We rolled Picks out to all Tinder users in September. ***This has helped drive more users to sign up for Gold subscription level, leading to an increase in ARPU since Gold comes at a premium price.*** This implementation of Picks resulted in increased ARPU but less of a conversation benefit. ***As is any new revenue feature, we will continue to refine our implementation and balance the trade-off between ARPU and the number of additional subscribers.***

- There are early signs that indicate ***our enhancements to the customer experience are leading to improved organic registrations due to stronger word-of-mouth marketing.***

(b) In the 11/7/2018 2018 Investor Call, Defendant Swidler also stated the following in prepared remarks:

- On Slide 10, you can see that ***average subscribers reached nearly 8.1 million in Q3, up 23% year-over-year. North America grew average subscribers 18% and international 29% year-over-year.***

- ***Tinder added 1.6 million average subscribers year-over-year, a 61% growth rate and 344,000 sequentially. Tinder's sequential subscriber growth was stronger than we'd expected as Gold continued to power the business. Picks*** [an incremental feature introduced as part of the Gold package] ***enhance Gold's appeal and product optimizations began to bear fruit.***

- ***Tinder Gold helped by Picks drove Tinder ARPU up 24% year-over-year and overall company higher by 6% year-over-year, up $0.03 to $0.57.***

- Looking to Slide 11, you can see that the ***subscriber and ARPU growth led to total revenue of $144 million for the quarter, year-over-year growth of 29%. Excluding FX impact of $8 million, total revenue would have been $452 million, 32% year-over-year growth. We demonstrated strength in direct revenue in Q3 with growth of 31%; North America grew direct revenue 25%; international, where Tinder comprises larger portion, was up 38%.***

101. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being

material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the

sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8 people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

102. On December 20, 2018, the *Wall Street Journal*'s website published a video interview (the "12/20/2018 Interview") with Defendant Ginsberg captioned, "*Match Group CEO Mandy Ginsberg: How I Work*." In it, Ginsberg said, in relevant part, "[I]t's really important for me to make sure that ***we do everything we can to provide safety and security for our users*** –

everything from one strike you're out to making sure that we put in processes and best practices across the organization to keep bad actors out."

103. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often

at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run

a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's

websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8 people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

104. On December 21, 2018, the *Wall Street Journal* published an article entitled "*The CEO Behind Tinder, OKCupid on the Future of Online Dating*" with a subtitle "*Match Group chief Mandy Ginsberg talks about her first year on the job, the Facebook threat and tackling loneliness through technology*" (the "12/21/2018 Article") that contained interview quotes by Defendant Ginsberg, as follows:

(a) In addressing Facebook's entry to online dating, Defendant Ginsberg said, "You can't underestimate Facebook, but ***I do feel confident that, with Tinder, our big growth engine***, people who are 21 years old are not going to be like, 'Oh, I'm going to get rid of my Tinder app in order to use Facebook.'"

(b) When asked to identify Match's "greatest potential," Ginsberg highlighted international markets and said, "***The biggest opportunity, frankly, is outside of the U.S. and Western Europe***."

(c) Asked to explain how Match's products changed in the "#MeToo" era, Defendant Ginsberg said, in relevant part, "I think a lot about the safety and security, in particular, of our

female users. ***It helps for us to have a portfolio [of matchmaking apps] because if there's bad behavior on one app, we can identify that user, we'll kick him off all the apps***. I do say 'him' because generally we see more bad behavior with men." The *Wall Street Journal* article was the original publication of this quote, providing the 'where and when' for Ginsberg's comments, and it was the source document from which *ProPublica* authors pulled the quote a year later for their piece published on December 2, 2019. Significantly, the *Wall Street Journal* article contains no statement by Ginsberg or Match regarding registered sex offenders being on Match's fee products or Match lacking a uniform screening protocol for such individuals. The *Wall Street Journal* article's context is devoid of any hedging language whatsoever concerning Defendant Ginsberg's reassuring statements concerning user safety on Match-branded websites and apps. Indeed, Ginsberg added, "When I started this year, I thought hard about what else should we do. I kicked off a safety advisory council. Tarana Burke, who founded the [original] #MeToo movement, is on it. They've been really helpful in identifying if there are any gaps or what we should be doing differently."

105. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported

members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together,

reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8 people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

106. On February 6, 2019, Match issued a press release (the "2/6/2019 Press Release"), which it filed with the SEC on February 6, 2019 as Exhibit 99.1 to Form 8-K signed by Defendant Swidler (the "2/6/2019 Form 8-K"), announcing its financial results for the Q4 and full year 2018. It stated as "Q4 2018 Highlights" that "***Total Revenue grew 21% over the prior year quarter to $457 million, driven by 17% Average Subscriber growth and 4% ARPU growth***" and "***Average Subscribers increased to 8.2 million, up from 7.0 million in the prior year quarter***."

107. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and

the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its

registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud

remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8 people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

108. On February 6, 2019, Yahoo! Finance issued an article (the "2/6/2019 Article") entitled "Match Beats Estimates as Tinder's Growth is Fueled by International Users." Within the article, CEO Ginsberg stated that 2018 marked "the ***best year in our history for shareholders***."

109. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said

should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold

through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would

have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8 people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

110. On February 7, 2019, Match held a conference call to discuss its financial results for Q4 and full year 2018 (the "2/7/2019 Investor Call"), during which Defendants Ginsberg and Swidler both spoke.

(a) During the 2/7/2019 Investor Call, Defendant Ginsberg stated the following in prepared remarks:

- Turning to Slide 5 and ***in its fourth year of monetization, Tinder nearly doubled direct revenue to $805 million. In 2018 Tinder added 1.2 million average subscribers and increased ARPU by 23%. Our strategy to increase the number of Gold subscribers was a key component of ARPU growth as was the continued ramp in a la carte purchases.***

- ***Tinder's top line remains impressive with 57% direct revenue growth, driven by 40% average subscriber growth and ARPU at 12% in the fourth quarter. Tinder exceeded our expectations for subscriber growth, primarily due to a number of ongoing product and merchandising optimizations that drove conversion wins, particularly in the back half of Q4.***

(b) Also in the 2/7/2019 Investor Call, Defendant Swidler stated in prepared remarks:

- On Slide 10, you can see that ***average subscribers reached over 8.2 million in Q4, up 17% year-over-year***.

- ***Tinder sequential subscriber growth was stronger than we had expected, as optimizations and merchandising changes drove higher conversion levels and more new subscribers and resubscribers***, offsetting much of the impact from a higher than normal number of expiring six and 12 month packages in Q4.

- ***In Q4, overall company ARPU was higher by 4% year-over-year, up $0.03 to $0.58***.

- Flipping to Slide 12. ***You can see that the 17% subscriber and 4% ARPU growth led to total revenue growth of 21%, with total revenue reaching $457 million for the quarter . . . . In terms of EBITDA, we saw year-over-year growth of 15% in Q4 to $176 million***.

111. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People

Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by

a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8

people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

112. On February 7, 2019, CNBC also broadcast a video interview (the "2/7/2019 Interview") with Defendant Ginsberg, excerpts of which were picked up and published the same day by other media outlets. During it, when asked what was behind the overall growth in membership and subscriptions, Ginsberg said, in relevant part, "***We really are seeing tremendous growth from Tinder***." When asked a follow up question about the business model, specifically the difference between the "Tinder Plus" and "Tinder Gold" subscription models, Ginsberg said:

> In terms of our business model, it's simple. You can go on Tinder and you can get a great free experience, but we offer features that you don't mind paying for. We had Plus, which was a subscription feature that enabled you to access a number of our premium features. Then ***about a year and a half ago, we introduced*** something called ***Gold***, ***which*** essentially ***gives you the ability to see who's liked you***. And, ***if someone says to you, do you want to see all the women who've liked you or all the men who've liked you, it's very hard to say no***. And we saw that people - ***the take rate on that Gold or that "likes you" feature was really high and that was priced at an even higher premium, another subscription tier***. So, what we saw is that not only were people happy to pay more for this feature, but ***we just saw more people taking the feature, and that's what's really driven a lot of the growth***.

113. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People

Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by

a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8

people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

114. On May 7, 2019, Match issued a press release ("the 5/7/2019 Press Release"), which that it filed with the SEC on May 7, 2019 as Exhibit 99.1 to Form 8-K signed by Defendant Swidler (the "5/7/2019 Form 8-K"), announcing its financial results for the Q1 2019. It stated as "Q1 2019 Highlights" that "***Total Revenue grew 14% over the prior year quarter to $465 million***," "***Total Revenue grew 14% over the prior year quarter to $465 million***," "***Average Subscribers increased 16% to 8.6 million, up from 7.4 million in the prior year quarter***," "***Tinder Average Subscribers were 4.7 million in Q1 2019, increasing 384,000 sequentially and 1.3 million year-over-year***," and "ARPU was flat over the prior year quarter; however, excluding foreign exchange effects, ***ARPU was $0.60, an increase of 4% over the prior year quarter***."

115. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said

should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold

through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would

have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8 people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

116. On May 8, 2019, Match held a conference call (the "5/8/2019 Investor Call") to discuss its financial results for the first quarter of 2019, during which both Defendants Ginsberg and Swidler spoke.

(a) During the 5/8/2019 Investor Call, Defendant Ginsberg stated that "***Tinder is driving very strong results***."

(b) Also during the 5/8/2019 Investor Call, Defendant Swidler stated the following in prepared remarks:

- On Slide 9, you can see that ***Tinder direct revenue grew 38% year-over-year in Q1 as our product optimization efforts in Q4 gave us momentum that continued into the new year…Given its scale, Tinder has lots of opportunity to optimize the user experience, which does two things, improves outcomes and matching, and drives more users to become paying subscribers, because they see value in being a payer.***

- ***Tinder subscribers grew 36% year-over-year in Q1 to just over 4.7 million. Tinder added 1.3 million subscribers year-over-year, and 384,000 subscribers sequentially…Tinder's ARPU is up 2% year-over-year on an as-reported basis, but on FX neutral basis, was up much more meaningfully.***

- On Slide 10, you can see that ***average subscribers across the company's brands reached over 8.6 million in Q1, up 16% year-over-year***.

- ***As reported ARPU for the company was stable overall at $0.58***. ***It was up 2% in North America***, but down 3% internationally because of negative impacts from FX. However, on an FX neutral basis, ***international ARPU is up 5% and overall company ARPU is up 4% or $0.02 to $0.60***.

- Flipping to Slide 11. ***You can see that the company's total revenue growth was 14% year-over-year, reaching $465 million of total revenue for the quarter***.

- ***North America grew direct revenue 12% driven by 10% subscriber growth and 2% ARPU growth, while international direct revenue increased 19% driven by 23% growth in subscribers and a 3% ARPU decline***

117. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People

Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by

a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8

people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

118. On May 8, 2019, Defendant Ginsberg appeared for an interview on CNBC's "Squawk Alley" to discuss Match's earnings and revenue (the "5/8/2019 CNBC Interview"). During it, Ginsberg stated that "***Tinder did drive a ton of growth this quarter. And we hit actually a big milestone, at the end of the quarter we had five million subscribers***."

119. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being

material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the

sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8 people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

120. On May 8, 2019, *Yahoo! Finance*'s "The First Trade" program broadcast a video interview with Defendant Swidler ("the 5/8/2019 Yahoo! Finance Interview") regarding Match's Q1 2019 reported results. The 5/8/2019 Interview included these exchanges:

(a) Regarding marketing to Tinder users to drive revenues, Swidler said:

> Q: So take us through the quarter a little bit, specifically Tinder. I'm curious on what you're doing to get more money out of the Tinder user. I know you've focused on boosts and some premium services. But what's the next big thing here?
>
> Swidler: Well you know Tinder is just a scaled platform around the world at this point in time. And there's just a lot of little things that we're doing right now that's driving more and more subscribers. ***We rolled out something called Tinder Gold about a year and a half ago now***. ***It's been a huge success***. And ***we're continuing to find ways to make that offering more compelling for users and have more people buy into Tinder Gold***. ***We're merchandising it better***. ***We're getting it in front of users more effectively***. ***And it's really working***.

(b) Regarding Match's competitive advantages to Facebook's new dating products, Swidler stated:

> Q: Facebook's dating service is now in 19 countries. It will launch in the U.S. later this year. What precautions are you taking ahead of this launch?
>
> Swidler: You know, Facebook so far really hasn't caused any impact on our existing business. They talked about it last May. They've been rolling it out slowly. We haven't seen any impact. So, we're watching them. Obviously, they're a huge player, a huge user base, especially internationally. So, we're not taking anything for granted. But we know this space incredibly well. ***We feel good about the comfort that users have with our products***. ***The features that we offer are really compelling for daters***. And we're driving our business. And we're watching Facebook, but we're really trying to do what we need to do. We know what that is. Obviously, Asia is going to be a big battlefront. A lot of the countries Facebook is talking about rolling out dating are in Asia. We're moving in Asia as well. And ***we feel great about our chances, just given how our products resonate with people who want to use the products for dating***.

121. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said

should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold

through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would

have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8 people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

122. In the July/August 2019 issue of the Harvard Business Review, Defendant Ginsberg wrote an article titled "*Match Group's CEO on Innovating in a Fast-Changing Industry*" ("the July/August 2019 HBR Article"). Among other things, it described Tinder's origin and growth, and included this description of Match's "freemium" model as fueling Tinder's soaring revenues:

> ***Most dating apps, including Tinder, have shifted to a "freemium" or paywall strategy***. Joining is free, and users get basic functionality. ***They can opt to pay for premium features such as seeing who likes you and swiping in another city***. ***Last year Tinder's revenue topped $800 million, demonstrating that many people are willing to pay for these features***.

123. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users

violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9

confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was

going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8 people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

124. On August 6, 2019, Match issued a press release (the "8/6/2019 Press Release"), which it filed with the SEC on August 6, 2019 as Exhibit 99.1 to Form 8-K signed by Defendant Swidler (the "8/6/2019 Form 8-K"), announcing its financial results for the second quarter of 2019. It stated as "Q2 2019 Highlights" that "***Total Revenue grew 18% over the prior year quarter to $498 million. Excluding foreign exchange effects, revenue would have grown 22%***," "***Average Subscribers increased 18% to 9.1 million, up from 7.7 million in the prior year quarter***," "***Tinder Average Subscribers were 5.2 million in Q2 2019, increasing 503,000 sequentially and 1.5 million year-over-year***," "***Operating income was $173 million, an increase of 15% over the prior year quarter***, and ***Adjusted EBTIDA increased 16% over the prior year quarter to $204 million***,"

and "***ARPU grew 2% over the prior year quarter to $0.58. Excluding foreign exchange effects, ARPU was $0.60, an increase of 5% over the prior year quarter***."

125. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often

at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run

a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from

Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8 people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

126. On August 7, 2019, Match held a conference call (the "8/7/2019 Investor Call") to discuss its financial results for Q2 2019, during which both Defendant Swidler stated:

- In Q2, ***Tinder subscribers grew 39% year-over-year to just over 5.2 million***. ***Tinder added nearly 1.5 million subscribers year-over-year and 503,000 subscribers sequentially***.

- On Slide 9, you can see that ***average subscribers across the company's brands reached over 9 million in Q2, up 18% year-over-year***.

- ***For the first time in our history, the number of international subscribers exceeded North American subscribers. We expect this trend to continue*** as our ***international growth efforts*** both ***at Tinder*** and elsewhere continue to gain steam.

- ***As-reported ARPU for the company was up $0.01 year-over-year to $0.58. It was up 4% in North America and up 1% internationally***. On an FX-neutral basis, ***international ARPU was up 7% and total company ARPU was up 5% year-over-year to $0.60***.

- Flipping to Slide 10, you can see the company's ***total revenue growth was 18% year-over-year, reaching $498 million of total revenue for the quarter***.

- ***North America grew direct revenue 13%, driven by 9% subscriber growth and 4% ARPU growth, while international direct revenue increased 27% driven by 27% growth in subscribers and a 1% ARPU increase***.

127. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among

the other seven colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on

a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud

was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8 people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

128. On September 10, 2019, Defendant Swidler attended the Deutsche Bank 2019 Technology Conference in Las Vegas, Nevada (the "9/10/2019 Conference"). During it, he stated the following:

> [I]f you look at Match Group's brands in Canada, which we think is the best analog to the U.S. market, it is our neighbor to the north. … It pays quite similarly to the U.S. ***And if you look at our Tinder, Match, OKCupid, Plenty of Fish brand in Canada, which are our primary brands in that market, you can see that subscriber growth has basically stayed on trend from the Facebook launch of dating back in November of '18 to today. You don't see any interruption or effect on subscriber growth in Canada from the Facebook launch in November '18***.
>
> And similarly, if you look at all the other countries, the other 18 countries where Facebook has rolled its dating product out ... ***We actually see acceleration of Tinder subscriber growth across that period***.
>
> [ ] ***But we don't see any deceleration of Tinder as a result of Facebook. And, in fact, we are very pleased with growth that we are showing on a year per year basis in all these other countries, even with Facebook dating in the market***.

129. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites

and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts

and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its

electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8 people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department

as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

130. On September 25, 2019, Match issued a press release entitled "Match Responds to FTC lawsuit" (the "9/25/2019 Press Release"). It stated the following:

> Fraud isn't good for business. That's why we fight it. ***We catch and neutralize 85% of potentially improper accounts in the first four hours, typically before they are even active on the site, and 96% of improper accounts within a day***.
>
> For nearly 25 years Match.com has been focused on helping people find love and fighting the criminals that try to take advantage of users. ***We've developed industry leading tools and AI that block 96% of bots and fake accounts from our site within a day and are relentless in our pursuit to rid our site of these malicious accounts.***

131. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the

Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation

into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1

said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8 people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

132. On November 5, 2019, Match issued a press release (the "11/5/2019 Press Release"), which it filed with the SEC on November 5, 2019 as Exhibit 99.1 to Form 8-K signed by Defendant Swidler (the "11/5/2019 Form 8-K"), announcing its financial results for Q3 2019 (the "11/5/2019 Press Release"). It stated as "Q3 2019 Highlights" that "***Total Revenue grew 22% over the prior year quarter to $541 million. Excluding foreign exchange effects, revenue would have grown 24%***," "***Average Subscribers increased 19% to 9.6 million, up from 8.1 million in***

the prior year quarter," "***Tinder Average Subscribers were 5.7 million in Q3 2019, increasing 437,000 sequentially and 1.6 million year-over-year***," "***Operating income was $177 million, an increase of 26% over the prior year quarter, and Adjusted EBITDA increased 25% over the prior year quarter to $206 million***," and "***ARPU grew 4% over the prior year quarter to $0.59. Excluding foreign exchange effects, ARPU was $0.60, an increase of 6% over the prior year quarter***."

133. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and

the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its

registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud

remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8 people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

134. On November 6, 2019, Match held a conference call to discuss its financial results for Q3 2019. During it, Defendant Swidler stated that "***we had another terrific quarter in Q3 with accelerated growth on top and bottom line, continued excellent performance at Tinder and improvement in non-Tinder subscriber trends***." Swidler also stated:

- On Slide 8, we review ***Tinder performance***, which ***continues to shine***. ***Q3 year-over-year growth in direct revenue of 49% accelerated from 2Q19 driven by 38% growth in average subscribers and 9% growth in ARPU.***

- On Slide 9, you can see that ***year-over-year growth in average subscribers across the company's brands accelerated in Q3, with overall average subscriber growth of 19%, 1 point better than in Q2 '19***. ***Year-over-year growth in North American and international subscribers also each accelerated from Q2. International subscriber growth was particularly strong, driven primarily by Tinder and Pairs***….

- ***Average subscribers for the quarter were just over 9.6 million, slightly***

> ***over half from outside of North America. We expect the shift to a greater proportion of international subscribers to continue as our international growth efforts at both Tinder and our other brands progress***.
>
> - ***This quarter, overall company ARPU was up $0.02 year-over-year to $0.59. On an FX-neutral basis, total company ARPU was up 6% to $0.60, and international ARPU was up 7%***.
>
> - Flipping to Slide 11, you can see that ***the company's Q3 total revenue was $541 million, for year-over-year growth of 22%, an acceleration of 4 points from Q2 '19***.

135. The foregoing misstatements were materially false and misleading because, as evidenced by both the CW statements set forth in §V.B. herein and the corrective revelations alleged in §V.D. herein, undisclosed to investors during the Class Period:

(a) Fraudulent and illegitimate accounts materially pervaded Match's branded websites and apps. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, stated that 15% of all Match.com membership registrations – 1 in 6 purported members – were fraudulent, a number that CW1, the Senior Manager of Financial Planning and Analysis for Match Group, said should be trusted. CW7, Tinder's Finance Director, said Tinder worked with the assumption that approximately 20% of all accounts and other account activity on Tinder – 1 in 5 purported members – were fraudulent. These fraudulent accounts impacted and inflated the financial results and performance metrics of Match's branded websites and apps both directly and indirectly. Directly, multiple CWs pegged the amount of paying accounts that were fraudulent as being material. CW11, one of six Trust & Safety Division members at Tinder who later worked in the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. CW5, a Fraud Investigator in Match's Fraud Department for seven years and

the third employee to delete over 1 million fraudulent accounts (having deleted up to 1.7 million such accounts), personally reviewed up to 2,200 accounts each day that were flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers, often at the 3-month or 6-month levels. CW5 said these metrics and percentages were consistent among the other seven colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW2 and CW5 said that the fraudsters upgraded to paid accounts to access enhanced functionalities. CW1 said that PlentyofFish had the biggest internally-reported problem with fraudulent accounts and the issue was a constant topic during the monthly forecast meeting with Match executives. CW1 and CW2 stated that Match's forecasts and operations reports, aside from those at PlentyofFish, did not adjust to exclude fraudulent accounts. Indirectly, CW2 and CW3 and the FTC Complaint stated that Match's branded websites and apps enticed non-paying users to upgrade to paid and premium memberships like Tinder Gold through "aggressive" marketing of purported messages, communications, and other activities from fraudulent and illegitimate accounts. The statements of CW1, CW2, CW9, CW10, taken together, reveal that once legitimate users upgraded, Match's branded websites and apps used deceptive terms, guarantees, and promotions to keep them stuck in a paid subscription, in the hopes that they would continue paying despite their dissatisfaction.

(b) Both the CWs and the Columbia Journalism Investigations ("CJI") investigation into the prevalence of sex offenders on dating apps and websites, reveal that Match's branded websites and apps either inadequately screened for sex offenders (in the case of Match.com) or did not screen for sex offenders and violent felons at all (in the case of Tinder and other brands). CW9 confirmed that Match.com did not prevent sex offenders from registering, opting to screen its

registered users instead. Yet, Match.com's screening system failed to screen any users who registered through an app store and in-app purchases, because the app store controlled the registration data, and screened directly registered users imperfectly at best, since Match.com intentionally failed to require the data pieces (full name, date of birth, address, etc.) required to run a sex offender registry search. Match.com's system still flagged 3% of all users as having a hit on a sex offender registry. CW3, CW8, and CW9 said that flagged users were manually searched by a small four-person team. CW10 said that Match.com did not screen for violent felons. CW11 said that Tinder did not perform any proactive screening for sex offenders and that the Trust & Safety Division only investigated potential sex offenders after receiving a complaint from another user, through a cumbersome process that did not even include a sex offender category among its electronic reporting options. CW8 confirmed that sex offenders were removed from Match.com every day. The CJI investigation also revealed that former Match employees on sites like Tinder and OKCupid received scant training and support for handling users' rape complaints and would have to devise their own ad hoc procedures for addressing complaints.

(c) Defendants Match, Ginsberg, and Swidler were focused on financial metrics, such as revenues, EBIDTA, PMC and ARPU, and on how to increase its membership base, rather than protecting users from being scammed or victimized by fraudulent accountholders, sex offenders, or other dangerous account users. Defendants Ginsberg and Swidler paid attention to fraud on the sites only if it created a variance in the forecasted PMC or ARPU of the website brands. CW1 said PlentyofFish's repeated downward adjustments of PMC/ARPU numbers to address fraudulent accounts caused "frustration" by Match executive leadership, particularly Ginsberg and Swidler, who were "tired of hearing about it." CW2 said there was an attitude of acceptance that there was going to be fraud on the websites and apps, and it was not viewed as urgent, so long as fraud

remained steady and did not suddenly spike. This focus on financial metrics meant that resources were pushed toward Tinder and away from the other brands and were deployed for revenue-generating activities rather than membership integrity, anti-fraud, or user safety. CW1 said that anti-fraud measures were not revenue-generating and that most of Match's websites, aside from Tinder, were treading water as far as profitability, such that additional funding to prevent fraud was not allocated. CW5 said that the work in the Fraud Department, consisting of just up to 8 people monitoring Match.com and the People Media Group collection of affinity brands, was "never ending," Department members worked 24/7 to manually review automatically flagged accounts, and CW5 personally deleted ~1.7 million fraudulent or illegitimate accounts, becoming the third employee to delete over 1 million such accounts. CW5 described the Fraud Department as "not very well-liked" and "the most hated team" within the company and as a "necessary evil as far as upper management was concerned," because "we did not help generate any money" and were actually "in the business of giving money back."

2. The Reported Results Fraud

136. Defendants also made a series of public statements and filings regarding Match's reported results that were materially false and misleading. These misstatements violated, among other things, Regulation S-K, Item 303, 17 C.F.R. §229.303(a)(3)(i)-(ii) and (b)(2).

137. On November 9, 2018, Match filed its Form 10-Q with the SEC related to the financial results for the third quarter of 2018 ("Q3 2018 Form 10-Q"), signed by Defendant Swidler and SOX certified by Defendants Ginsberg and Swidler. It stated that for the three months ended September 30, 2018 compared to the three months ended September 30, 2017, "[i]nternational Direct Revenue grew $54.7 million, or 38%, in 2018 versus 2017, primarily driven by 29% growth in Average Subscribers and a 7% increase in ARPU. North America Direct Revenue grew $46.8

million, or 25%, in 2018 versus 2017, driven by 18% growth in Average Subscribers and 6% growth in ARPU." It also stated that for the nine months ended September 30, 2018 compared to the nine months ended September 30, 2017, "[i]nternational Direct Revenue grew $188.3 million, or 50%, in 2018 versus 2017, primarily driven by 34% growth in Average Subscribers and a 13% increase in ARPU. North America Direct Revenue grew $126.5 million, or 23%, in 2018 versus 2017, driven by 18% growth in Average Subscribers and 4% growth in ARPU."

138. On February 28, 2019, Match filed its Form 10-K with the SEC related to Match's financial results for the fourth quarter and full year of 2018 ("2018 Form 10-K"), signed and SOX certified by Defendants Ginsberg and Swidler. It stated that for the year ended December 31, 2018 compared to the year ended December 31, 2017, "[i]nternational Direct Revenue grew $234.8 million, or 43%, in 2018 versus 2017, driven by 31% growth in Average Subscribers, and a 10% increase in ARPU. North America Direct Revenue grew $161.1 million, or 22%, in 2018 versus 2017, driven by 17% growth in Average Subscribers, and a 4% increase in ARPU."

139. On May 9, 2019, Match filed its Form 10-Q with the SEC related to its financial results for the first quarter of 2019 ("Q1 2019 Form 10-Q"), signed by Defendant Swidler and SOX certified by Defendants Ginsberg and Swidler. It stated that for the three months ended March 31, 2019 compared to the three months ended March 31, 2018, "[i]nternational Direct Revenue grew $34.8 million, or 19%, in 2019 versus 2018, primarily driven by 23% growth in Average Subscribers, partially offset by a 3% decrease in ARPU. North America Direct Revenue grew $26.4 million, or 12%, in 2019 versus 2018, driven by 10% growth in Average Subscribers and 2% growth in ARPU."

140. On August 9, 2019, Match filed its Form 10-Q with the SEC related to Match financial results for the second quarter of 2019 ("Q2 2019 Form 10-Q"), signed by Defendant

Swidler and SOX certified by Defendants Ginsberg and Swidler. It stated that for the three months ended June 30, 2019 compared to the three months ended June 30, 2018, "[i]nternational Direct Revenue grew $50.2 million, or 27%, in 2019 versus 2018, primarily driven by 27% growth in Average Subscribers, and a 1% increase in ARPU. North America Direct Revenue grew $29.3 million, or 13%, in 2019 versus 2018, driven by 9% growth in Average Subscribers and 4% growth in ARPU." It added that for the six months ended June 30, 2019 compared to the six months ended June 30, 2018, "[i]nternational Direct Revenue grew $85.0 million, or 23%, in 2019 versus 2018, primarily driven by 25% growth in Average Subscribers, partially offset by a 1% decrease in ARPU. North America Direct Revenue grew $55.8 million, or 13%, in 2019 versus 2018, driven by 10% growth in Average Subscribers and 3% growth in ARPU. Indirect Revenue decreased $6.8 million."

141. On November 7, 2019, Match filed its Form 10-Q with the SEC related to its financial results for the third quarter of 2019 ("Q3 2019 Form 10-Q"), signed by Defendant Swidler and SOX certified by Defendants Ginsberg and Swidler. It stated that for the three months ended September 30, 2019 compared to the three months ended September 30, 2018, "[i]nternational Direct Revenue grew $64.2 million, or 32%, in 2019 versus 2018, primarily driven by 29% growth in Average Subscribers, and a 3% increase in ARPU. North America Direct Revenue grew $35.2 million, or 15%, in 2019 versus 2018, driven by 10% growth in Average Subscribers and 5% growth in ARPU." It added that for the nine months ended September 30, 2019 compared to the nine months ended September 30, 2018, "[i]nternational Direct Revenue grew $149.2 million, or 26%, in 2019 versus 2018, primarily driven by 26% growth in Average Subscribers and a 1% increase in ARPU. North America Direct Revenue grew $91.0 million, or 14%, in 2019 versus

2018, driven by 10% growth in Average Subscribers and 4% growth in ARPU. Indirect Revenue decreased $8.6 million."

142. The misstatements in the preceding five paragraphs were materially false and misleading because, as demonstrated at length by the CW statements set forth herein, undisclosed to investors during the Class Period, they reported Match's financial results and metrics, including without limitation revenues, earnings, PMC, ARPU, and conversions of unpaid to paid memberships, as well as positive or insufficiently negative reports of Match's underlying business and its branded websites and apps, without disclosing that the reported results and metrics were generated through inclusion of widespread accounts, including paid subscriptions, by scammers, fraudsters, "bots," sex offenders, and other dangerous site users, and that Match faced material undisclosed risks due to this underlying misconduct. It was materially false and misleading to reference such positive results and metrics, to refute or minimize potentially significant concerns like analyst questions over user safety, investigative reports over sex offender usage on Match apps and websites, or, when it was finally disclosed, the FTC's investigation, while omitting disclosure of the underlying misconduct and risks set forth herein, including those evidenced by the CW accounts alleged in §V.B. *supra* and the revelations set forth in §V.D. *infra*, specifically among them the inclusion of fraudulent or illegitimate accounts in Match's reported results, and Match's basing its marketing of subscription products like Tinder Gold on the existence and activities of those fraudulent and illegitimate accounts, resulting in legitimate users wrongly being enticed to convert from non-paying to paying, all of which both inflated the positive metrics and results disclosed and surpassed in severity any risks actually disclosed elsewhere in Match's public statements. As such, these misstatements and omissions violated, *inter alia*, Regulation S-K, Item 303, 17 C.F.R. §229.303(a)(3)(i)-(ii) and (b)(2).

D. PARTIAL CORRECTIVE DISCLOSURES INCREMENTALLY REVEALED THE FRAUDS

143. Interspersed with the foregoing misstatements were a series of partial corrective disclosures that incrementally revealed aspects of Defendants' fraud, which caused the inflation to be removed in stages from Match's stock price.

144. On February 28, 2019, Match filed its 2018 10-K, which revealed the following previously undisclosed facts to investors, stating:

> ***In March 2017, the Federal Trade Commission ("FTC") requested information and documents in connection with a civil investigation regarding certain business practices of Match.com. In November 2018, the FTC proposed to resolve its potential claims relating to Match.com's marketing, chargeback and online cancellation practices via a consent judgment mandating certain changes in the company's business practices, as well as a payment in the amount of $60 million.*** Match Group believes that the FTC's legal challenges to Match.com's practices, policies, and procedures are without merit and is prepared to vigorously defend against them.

145. On this news, which was muted by Match's false and misleading statements within the same filing, as discussed *supra*, Match's stock price fell $.40, or .72%, from its February 27, 2019 closing price of $55.78 to close at $55.38 on February 28, 2019.

146. On August 9, 2019, Match filed its Q2 2019 Form 10-Q, which was signed by Defendant Swidler and SOX certified by Defendants Ginsberg and Swidler. In addition to the previous disclosures regarding the FTC's investigation into Match's business practices, it disclosed that the FTC was asserting claims against Match based on its investigation stating:

> ***On August 7, 2019, the FTC voted to assert claims against the Company and referred the matter to the U.S. Department of Justice ("DOJ"). The Company expects to continue discussions with the FTC and DOJ. In the event no settlement is reached and litigation ensues, the amount sought may be substantially higher than the amounts discussed in settlement.*** Match Group believes that the FTC's claims regarding Match.com's practices, policies, and procedures are without merit and is prepared to defend vigorously against them

147. On this news, Match's stock price fell $1.54, or 1.8%, on high volume, from its August 8, 2019 closing price of $87.17 to close at $85.63 on August 9, 2019.

148. Over the weekend, news of the FTC's assertion of claims against Match leaked to investors. Match's stock price continued its downward decline falling another $2.99, or 3.5%, from its August 9, 2019 closing price of $85.63 to close at $82.64 on August 12, 2019 (the next trading day).

149. On September 25, 2019, the FTC announced that it had sued Match.com for, among other things, using artificial love interest ads to deceive consumers into buying or upgrading subscriptions, failing to resolve disputed charges, and intentionally making it difficult to cancel subscriptions. In a press release announcing the lawsuit, the FTC stated, in relevant part:

> Specifically, when nonsubscribers with free accounts received likes, favorites, emails, and instant messages on Match.com, they also received emailed ads from Match encouraging them to subscribe to Match.com to view the identity of the sender and the content of the communication.
>
> The FTC alleges that millions of contacts that generated Match's "You caught his eye" notices came from accounts the company had already flagged as likely to be fraudulent. By contrast, Match prevented existing subscribers from receiving email communications from a suspected fraudulent account.
>
> Many consumers purchased subscriptions because of these deceptive ads, hoping to meet a real user who might be "the one." The FTC alleges that instead, these consumers often would have found a scammer on the other end. According to the FTC's complaint, consumers came into contact with the scammer if they subscribed before Match completed its fraud review process. If Match completed its review process and deleted the account as fraudulent before the consumer subscribed, the consumer received a notification that the profile was "unavailable." In either event, the consumer was left with a paid subscription to Match.com, as a result of a false advertisement.
>
> * * *
>
> Hundreds of thousands of consumers subscribed to Match.com shortly after receiving communications from fake profiles. According to the FTC's complaint, from June 2016 to May 2018, for example, Match's own analysis found that consumers purchased 499,691 subscriptions within 24 hours of receiving an advertisement touting a fraudulent communication.

* * *

> The FTC also alleges Match deceptively induced consumers to subscribe to Match.com by promising them a free six-month subscription if they did not "meet someone special," without adequately disclosing that consumers must meet numerous requirements before the company would honor the guarantee.

* * *

> Finally, the FTC alleges that Match violated the Restore Online Shoppers' Confidence Act (ROSCA) by failing to provide a simple method for a consumer to stop recurring charges from being placed on their credit card, debit card, bank account, or other financial account. Each step of the online cancellation process— from the password entry to the retention offer to the final survey pages—confused and frustrated consumers and ultimately prevented many consumers from canceling their Match.com subscriptions, the FTC contends. The complaint states that Match's own employees described the cancellation process as "hard to find, tedious, and confusing" and noted that "members often think they've cancelled when they have not and end up with unwanted renewals."

150. On this news, Match's share price fell $1.39, or nearly 2%, from its September 24, 2019 closing price of $72.83 to close at $71.44 on September 25, 2019, on unusually high trading volume.

151. On November 6, 2019, Match held an earnings call with analysts and investors (the "11/6/2019 Investor Call"), on which Defendants Ginsberg and Swidler participated. During this call, they disclosed that revenues were impacted by increased legal costs in 2019 and 2020 due to 3 lawsuits. During prepared remarks, Defendant Swidler stated that Match expected $25 million in incremental legal costs for 4Q2019 and that the higher legal costs were impacting Match's margin for full-year 2019. In the question-and-answer portion of the Investor Call, Defendant Swidler provided more detail regarding the legal expenses Match expected to incur in 2019 and 2020, stating:

> ***On the legal side, if you look at the trends in legal, our legal costs this year are jumping significantly from last year. In 2018, we had about $15 million of legal fees. This year, we've got about $40 million more expected for the year, so close to $55 million, so it's a significant jump in '19, and then our numbers for 2020 include additional legal fees***

> ***probably in the neighborhood of about $15 million or so. The jump is pretty significant from '18 to '19, and then incrementally from '19 to '20.***
>
> Now, we don't view those as discretionary. We are involved in ***three significant lawsuits*** and we are pursuing those with top flight lawyers because in one of the cases, Bumble, we think they've infringed on our patents and we're expecting to be compensated for that, so we've been pursuing that litigation. On the other two, ***one related to the FTC and DOJ investigation, we think the claims that have been made in that case are meritless and we are going to defend ourselves against that vigorously, so that is increasing our legal costs in 2020.*** It started now in late '19, and it's going to take place over the course of 2020.

152. On this news, Match's share price fell $1.73, or 2.5%, from its November 5, 2019 closing price of $68.77 to close at $67.04 on November 6, 2019, on unusually high trading volume.

153. On December 2, 2019, Columbia Journalism Investigations ("CJI") published the findings of its 16-month investigation analyzing more than 150 incidents of sexual assault involving dating apps, culled from a decade of news reports, civil lawsuits, and criminal records. CJI's article disclosed that Match screens for sexual predators on Match.com, but not on any of its other "free products" such as Tinder, OkCupid or PlentyofFish. The article stated, in part:

> For nearly a decade, [Match.com] has a policy of screening customers against government sex offender registries. But over this same period***, as Match evolved into the publicly traded Match Group and bought its competitors, the company hasn't extended this practice across its platforms — including PlentyofFish, its second most popular dating app. The lack of a uniform policy allows convicted and accused perpetrators to access Match Group apps and leaves users vulnerable to sexual assault.***
>
> ****
>
> ***Today, Match Group checks the information of its paid subscribers on Match[.com] against state sex offender lists. But it doesn't take that step on Tinder, OkCupid or PlentyofFish — or any of its free platforms.*** A Match Group spokesperson told CJI the company cannot implement a uniform screening protocol because it doesn't collect enough information from its free users — and some paid subscribers — even when they pay for premium features. ***Acknowledging the limitations, the spokesperson said, "There are definitely registered sex offenders on our free products."***
>
> ****

> ***Interviews with more than a dozen former Match Group employees — from customer service representatives and security managers at OkCupid to senior executives at Tinder*** — paint a different picture. Most left on good terms; indeed, many told CJI they're proud of the successful relationships their platforms have facilitated. But they criticize the lack of companywide protocols. Some ***voice frustration over the scant training and support they received for handling users' rape complaints. Others describe having to devise their own ad hoc procedures. Often, the company's response fails to prevent further harm, according to CJI interviews with more than 100 dating app users, lawmakers, industry experts, former employees and police officers; reviews of hundreds of records; and a survey of app users.***
>
> ***Even the screening policy on the one site that checks registries, Match, is limited. The company's spokesperson acknowledges that the website doesn't screen all paid subscribers.***

154. The article also presented a host of specific cases in which victims of sexual assault or rape who used one of Match's branded websites stated that they informed the various website brands of the sexual predators on the sites, but in many instances, they received no response and/or the profiles of the assaulters were still visible to the victims indicating Match took no action.

155. On this news, Match's share price fell $2.06, or nearly 3%, from its November 29, 2019 closing price of $70.48 to close at $68.42 on December 2, 2019, on high trading volume.

156. On January 31, 2020, the House Committee on Oversight and Reform's Subcommittee on Economic and Consumer Policy issued a press release announcing that it had launched an investigation into reports about underage use of dating applications, and inappropriately selling or sharing personal data. The press release stated that letters were sent to Match, along with 3 other dating apps, seeking information related to, among other things, recent reports that numerous dating apps have failed to effectively screen out underage users. The press release quoted Chairman of the Subcommittee Raja Krishnamoorthi who stated:

> Our concern about the underage use of dating apps is heightened by reports that many popular free dating apps permit registered sex offenders to use them, while the paid versions of these same apps screen out registered sex offenders. Protection from sexual predators should not be a luxury confined to paying customers.

157. The letter sent to Match was linked to the press release and, in part, requested documents an information regarding policies and procedures relating to whether the companies allowed registered sex offenders or those convicted of violent crimes to use their products or service, including how they determine if users are registered sex offenders or have been convicted of violent crimes and what actions they take when they discover that they are. The companies were requested to produce documents by February 13, 2020. No further updates have been provided to date.

158. On this news, Match's share price fell $2.83, or 3.5%, from its January 30, 2020 closing price of $81.05 to close at $78.22 on January 31, 2020, on high trading volume.

159. As a result of Defendants' wrongful acts and omissions, and the precipitous decline in the market value of Match's securities, Plaintiff and other Class members have suffered significant losses and damages.

E. POST-CLASS PERIOD FACTS UNDERSCORE ONGOING RISKS FOR MATCH FROM THE UNDERLYING MISCONDUCT AT ISSUE

160. FTC and Congressional investigations remain ongoing. In February 2020, 11 members of the U.S. House Energy and Commerce Committee sent a letter to Match Group President Shar Dubey calling on Match to check users against sex offender registries and to disclose efforts to respond to reports of sexual violence resulting from users meeting through Match Group services. A forthcoming proposed Online Consumer Protection Act would force dating apps to be more transparent with users about terms of service, enforce rules designed to prevent fraud and abuse, and hold them accountable for failure to do so. The FTC's action against Match seeks equitable monetary relief under Section 13(b) of the FTC Act and was stayed, pending the outcome of the appeal in *FTC v. Credit Bureau, Ctr., LLC*, No. 19-825, 141 S. Ct. 194 (2020)

and *AMG Capital Mgmt., LLC v. FTC*, No. 19-508, 141 S. Ct. 194 (2020), which concern whether Section 13(b) permits the FTC to seek monetary as well as injunctive relief.

F. ADDITIONAL FACTS PROBATIVE OF SCIENTER

161. The following facts support a strong inference of scienter, when viewed holistically and in the context of this amended pleading. While the Court has previously addressed certain of these facts in its prior Order (Dkt. No. 50), some are realleged herein, modified or unmodified, for purposes of reexamination, in a holistic analysis, with additional and/or enhanced allegations.

1. Defendants Ginsberg's and Swidler's Knowledge or Reckless Disregard of Red Flags Demonstrates Scienter

162. The CWs attest to Defendants Ginsberg's and Swidler's direct knowledge as to key aspects of the fraud at issue, including that between 15% and 20% of the users on Match's websites and apps were perpetrators of fraud and that a "significant percentage" of blocked accounts were paid subscribers.

163. Tinder's Director of Analytics told CW7 that Tinder worked with the assumption that 20% of all Tinder accounts and account activity were fraudulent and/or bots, and CW7, Tinder's Finance Director, did not adjust any reported performance or financial metrics to account for that fact, despite even knowing that some premium subscriptions were scammers looking to take advantage of advanced features to further their frauds. CW1 stated that Dubey, Match's then-President and current CEO, was very hands-on and in the weeds with Tinder's operations during CW1's tenure at Match and at one point, operated out of Tinder's offices exclusively for a period of six months. CW1 said that Dubey would have been aware of any red flags with Tinder's operations, such as bad actors on Tinder's site, and would have relayed them to Defendant Ginsberg, with whom she interacted daily, and to Defendant Swidler, with whom she interacted at least two days a week.

164. CW2, Match.com's Senior Finance Manager at its Dallas headquarters, did a Finance Department analysis based on a comparison of the raw number of registrations on any given day against how many of those members were removed by the Fraud Department seven days later and found that 15% of all Match.com membership registrations were fraudulent. CW2 added that the fraudulent registrations percentage remained close to 15% at least throughout CW2's entire 3-year tenure. When informed that CW2 said that 15% of Match.com registrations were fraudulent, CW1 said that CW2 should be trusted to know that number because CW2 spent about a week and a half every month preparing the detailed forecast report and looking at all of the financials for Match.com. CW1 also stated that Ginsberg would have been particularly aware of the statistics on the number of fraudulent accounts on the Match.com site given her prior role as Match.com CEO.

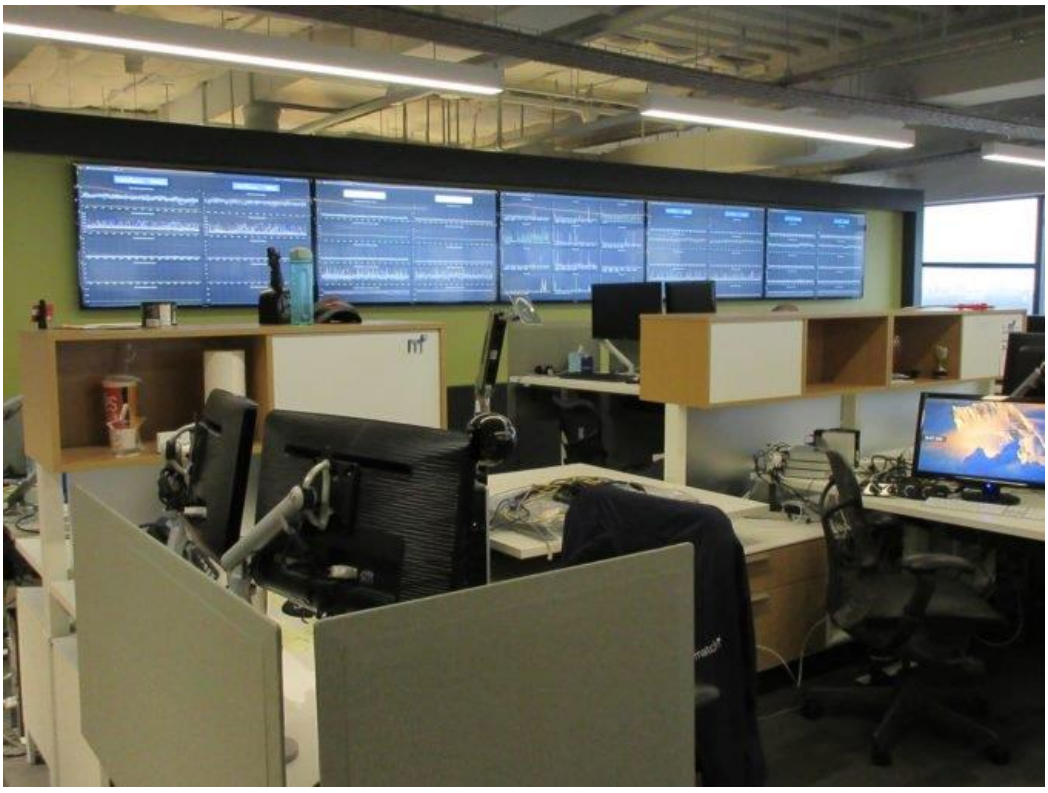
165. Other CWs corroborated the statements of CW1, CW2, and CW7. When informed of them, CW11, who was one of six Trust & Safety Division members at Tinder before transferring to the Customer Service Division, expressed the view that 15%-20% of fake, fraudulent, and bad actor accounts were paid subscriptions, including bots, users posing as another person, accounts using stolen credit cards to pay for subscriptions, scammers trying to defraud other users, and other users violating site rules. Blocked from disclosing actual figures by a nondisclosure agreement, CW13 nevertheless confirmed CW7's statement that Tinder had internal estimates of the amount of its existing accounts that were fake, fraudulent, or bad actors that the anti-fraud team had not caught, which estimates were tracked on an ongoing basis and based on and fluctuated with the number of such accounts that were caught. CW13 added, "There's knowledge of that."

166. CW5, a long-time employee who worked seven years as a Senior Fraud Investigator in Match's Fraud Department and personally deleted up to 1.7 million accounts (the third employee

to surpass the 1 million deletions mark), said that every day, CW5 reviewed up to 2,200 accounts flagged for potential fraudulent activity, blocked a low- to mid-40 percent for actually engaging in fraudulent activity, and found that a "significant percentage" of those blocked accounts were paid subscribers – metrics and percentages that were consistent among CW5's seven other colleagues in the Fraud Department, which oversaw Match.com and the People Media Group collection of affinity brands. CW5 explained that the high percentage of fraudulent accounts was because any fraudster wanting to actually communicate with victims, by sending messages and seeing responses, needed to have a paid subscription account to do so. CW5 added that although Match.com offered subscriptions as low as 1-month, many fraudsters actually paid for 3-month and 6-month subscriptions to avoid detection and create some facial legitimacy for their account. CW5 was confident that the company tracked the percentage of fraudulent accounts that were paid, stating, "I do know for sure that Match as a company – they have those numbers. I know they do. The higher ups – they want to know that info. It was something that they always wanted to keep track of."

167. CW1 said the brand PlentyofFish had the biggest internally reported problem with fraudulent accounts, and the issue became a constant topic during the monthly forecast meeting with Match executives, including Defendants Ginsberg and Swidler, who were particularly frustrated with the effects of fighting fraud at that one website on its forecasted PMC and ARPU. CW1 clarified that Ginsberg and Swidler appeared frustrated that PlentyofFish kept reducing forecasts due to removal of fake / fraudulent accounts and were "tired of hearing about it." CW1 added that due to Tinder's outsized impact on Match's revenues, Tinder received more resources for operations than smaller apps like PlentyofFish, which could impact the amount of resources they could dedicate to identifying and removing fake, fraudulent, and bad actor accounts.

168. Evidence of the fraud rampant on Match's websites was also prevalent at Match's company headquarters. CW1 stated that policies for fraud detection were set across all website brands and decided upon by the board of directors, with Defendant Ginsberg, Defendant Swidler, and Dubey weighing in. CW4 added that everyone in the headquarters building had knowledge of the number of fraudulent accounts and that fraud was a frequent topic at the twice weekly operations meetings. CW6, CW9, and CW1 described a wall of screens on the main floor of Match's Dallas headquarters (shown below) that would display, among other things, website usage levels and traffic patterns. CW6 stated that an unusual traffic spike would be visible and could indicate the presence of "bots" or that fraudsters had found a new way to avoid detection on the site. The wall of screens was highly visible in the open concept design floorplan of Match's headquarters, which is where Defendant Ginsberg's office, the main entrance, large conference rooms, café/break room, and other communal gathering spots were located.



169. CW5 described an internal database at Match.com that tracked how many account profiles each Fraud Department investigator reviewed each day, how many were blocked for fraudulent activity, and a breakdown of blocked accounts into subcategories as to why the account was flagged, including reasons such as another user's email, the account's photo, or an internal algorithm system. Per CW5, the database was accessible at any time, permitted viewing of the numbers for all Fraud Department investigators, and could be used to generate reports showing CW5's metrics or those of all the investigators in the Fraud Department.

170. Given all the foregoing, Defendants Ginsberg and Swidler had a duty to disclose these undisclosed facts regarding fraudulent accounts and their impacts on Match's operations and reported results, both direct impacts due to inflating subscription revenues and indirect impacts due to Match's deploying "aggressive" marketing to entice legitimate, non-paying users to convert to paid subscriptions, like Tinder Gold, by promoting to them reactions and messages from fraudulent accounts that could only be viewed / read on a paid subscription, which duty arose once they decided to speak publicly about issues regarding Match's marketing, consumer satisfaction and customer experience, subscription levels and revenues, and user levels and growth, *e.g.*, in the 11/6/2018 Press Release, 116/2018 Form 8-K, 11/7/2018 Investor Call, Q3 2018 Form 10-Q, 12/21/2018 Article with Ginsberg interview excerpts, 2/6/2019 Press Release, 2/6/2019 Form 8-K, 2/6/2019 Article, 2/7/2019 Investor Call, Ginsberg's 2/7/2019 Interview, 2018 Form 10-K, 5/7/2019 Press Release, 5/7/2019 Form 8-K, Ginsberg's /8/2019 CNBC Interview, Swidler's 5/9/2019 Yahoo! Finance Interview, Q1 2019 Form 10-Q, July/August HBR Article, 8/6/2019 Press Release, 8/6/2019 Form 8-K, 8/7/2019 Investor Call, Q2 2019 Form 10-Q, 9/10/2019 Conference, 11/5/2019 Form 8-K, 11/6/2019 Investor Call, and Q3 2019 Form 10-Q. They violated that duty by making these misstatements and omissions.

171. Defendants Ginsberg and Swidler also ignored red flags regarding the presence of sex offenders, felons, and dangerous users on Match's branded apps and websites. A 2011 lawsuit by a woman claiming sexual assault by someone she met on Match.com prompted Match to implement a system to screen memberships against a national sex offender registry. However, the system had glaring, undisclosed loopholes and vulnerabilities, such as the inability to run such searches on users who registered via app stores and in-app purchases and the intentional failure by Match.com, due to privacy and intrusiveness concerns, to request the fulsome information from registering site users – such as full name, date of birth, accurate mailing address, etc. – that would permit successful sex offender registry searches. CW9 stated that Match.com did not prevent sex offenders from registering in the first place, and CW10 said that Match.com did not screen at all for violent felons. Notwithstanding these significant limitations, Match.com still flagged 3% of the subset of registered users that could be searched against a registry, at which point a tedious, manual process was undertaken by a thinly-staffed, four-person team described by CW3, CW8, and CW9 – which still resulted in the removal of sex offenders daily. Despite all these red flags, CW11 confirmed that Match implemented no sex offender screening whatsoever on its fastest-growing, highest-earning brand, Tinder, from which sex offenders were removed by the Trust & Safety staff only after being reported by members via a cumbersome process that did not even include a "sex offender" category for a report. CW11 also confirmed that Tinder had no barriers to registration for sex offenders, and Tinder registration did not even require a user to input his actual name. CW1 confirmed that Defendants Ginsberg and Swidler would have been aware of red flags at Tinder because Match's then-President (and now-CEO) Shar Dubey spent three to four days a week at Tinder for a six-month period in 2017, during which time she interacted with

Defendant Ginsberg daily and Defendant Swidler several times weekly, as Dubey relayed to CW1 during telephonic meetings in which they both participated.

172. Defendants Ginsberg and Swidler had a duty to disclose these undisclosed facts regarding sex offenders and violent felons on Match's branded apps and websites and the limited screening or complete lack of screening for such users, which duty arose once they decided to speak publicly and specifically about issues regarding user safety, *e.g.*, in Ginsberg's 12/20/2018 Interview, the 12/21/2018 Article with Ginsberg interview excerpts, and the 9/25/2019 Press Release. They violated that duty by making these misstatements and omissions.

173. The CWs also explained some impacts of fraudulent accounts on Match's reported results and metrics, both directly and indirectly as enticements to entice legitimate non-paying users to upgrade to paid subscriptions when they otherwise would not have done so. CW5 said that Match.com automatically refunded the full subscription fees for fraudulent accounts that were blocked and removed, even those with longer terms of 6-months or even 1-year, as so many of them were paid by stolen credit cards. CW5 said that, as a result of reducing rather than increasing revenues, the Fraud Department was viewed as a "necessary evil" [by] upper management," was "not very well-liked" within the company, and was the "most hated team." CW2 described Match.com's use of fraudulent accounts to drive conversions of legitimate users from paying to non-paying. CW2 stated that Match.com sent "aggressive" emails to non-subscribers promoting "all messages, even if they were fraudulent." CW2 said that "definitely over 30%" of paying memberships were non-paying members who converted to subscribers after receiving a notification that they had a message they could not read unless they paid for a membership and that "a percentage of the messages marketed to non-subscribers were fraudulent." CW3 said a frequent subscriber complaint was that they received a marketing email stating that people liked

them, prompting them to subscribe, only to learn that those "liking" accounts were not real or had been removed. CW10, CW8, and CW4 all described marketing emails sent to non-paying customers telling them that they had messages waiting for them and prompting them to subscribe, only to find those messages missing.

174. All the foregoing facts evidence Defendants Ginsberg's and Swidler's knowledge of the facts rendering their Class Period misstatements and omissions materially false and misleading, or at worst, their reckless disregard for those facts.

2. Defendants Ginsberg's and Swidler's Suspicious, Widespread Insider Trading During the Class Period Evidences Scienter

175. Scienter is further evidenced by the Class Period transactions in Match stock, options, and stock-related units by Defendants Ginsberg and Swidler, suspicious in timing and amount, which permitted them to accumulate tens of millions of dollars in ill-gotten gains during the fraud alleged herein. Specifically, such sales included the following:

(a) Defendant Ginsberg's Class Period Transactions

Entering the Class Period, Defendant Ginsberg held 19,349 shares of common stock, 1, 424,402 stock options, and 266,667 RSUs. Defendant Ginsberg's transactions during the Class Period were as follows:

Stock Options Transactions					
Transaction Date	**Options Grants / Exercises**	**Shares**	**Vesting Date**	**Strike Price**	**Funds Spent / Gained**
5/30/2019	Exercise of Options [*expiration date 9/17/2025*]	136,711	1/4 each on 12/31/2016; 12/31/2017; 12/31/2018; 12/31/2019	$14.6952	($2,008,995)
5/30/2019	Exercise of Options	65,667	1/4 each on 12/21/2016; 12/21/2017;	$13.2295	($868,742)

	[*expiration date 12/21/2025*]		12/21/2018; 12/21/2019		
5/30/2019	Exercise of Options [*expiration date 12/21/2025*]	45,528	1/3 each on 12/21/2016; 12/21/2017; 12/21/2018; 12/21/2019	$13.2295	($602,313)
Sub-Total Options from Grants/Compensation				**Cost**	($0)
Sub-Total Options Exercised		247,906		**Cost**	($3,480,050)
RSU Transactions					
Transaction Date	**Unit Grants / Exercises**	**Units**	**Vesting Date**	**Price**	**Funds Spent / Gained**
12/21/2018	Exercise of RSUs	(35,021)	1/3 each on 12/21/2017; 12/21/2018; 12/21/2019	$0	$0
2/9/2019	Exercise of RSUs	(52,534)	1/2 each on 2/9/2019; 2/9/2020	$0	$0
12/21/2019	Exercise of RSUs	(35,024)	1/3 each on 12/21/2017; 12/21/2018; 12/21/2019	$0	$0
Sub-Total Grants of RSUs		(122,579)		**Cost**	($0)
Sub-Total Exercises of RSUs		0		**Proceeds**	$0
Stock Transactions					
Transaction Date	**Purchases / Sales**	**Shares**		**Price**	**Funds Spent / Gained**
12/21/2018	Acquired by RSU exercise	35,021		$0	$0
12/21/2018	Sale	(13,782)		$40.0500	$551,969
2/9/2019	Acquired by RSU exercise	52,534		$0	$0
2/9/2019	Sale	(18,049)		$56.6100	$1,021,754

5/30/2019	Acquired by options exercise	136,711	*See above*	*See above*
5/30/2019	Acquired by options exercise	65,667	*See above*	*See above*
5/30/2019	Acquired by options exercise	45,528	*See above*	*See above*
5/30/2019	Sale	(119,879)	$69.0520	$8,277,885
5/30/2019	Sale	(128,027)	$69.2612	$8,867,310
12/21/2019	Acquired by RSU exercise	35,024	*See above*	*See above*
12/21/2019	Sale	(13,783)	$79.8600	$1,100,710
Sub-Total Stock Sales		(293,520)	**Proceeds**	**$19,819,628**

Totals	**Shares Purchased**	**0**	**Transaction Costs**	**$0**
	Shares Acquired by Options Exercise	**247,906**	**Transaction Costs**	**($3,480,050)**
	Shares Acquired by RSU Exercise	**122,579**	**Transaction Costs**	**($0)**
	Shares Sold	**(293,520)**	**Transaction Proceeds**	**$19,819,628**
		Net Gain to Defendant Ginsberg		**$16,339,578**

(b) Defendant Swidler's Class Period Transactions

Entering the Class Period, Defendant Swidler held 63,090 shares of common stock, 798,345 stock options, and 175,000 RSUs. Defendant Swidler's transactions during the Class Period were as follows:

Stock Options Transactions					
Transaction Date	**Options Grants / Exercises**	**Shares**	**Vesting Date**	**Strike Price**	**Funds Spent / Gained**
2/11/2019	Exercise of Options [*expiration date 9/17/2025*]	32,119	1/4 each on 2/9/2018; 2/9/2019; 2/9/2020; 2/9/2021	$17.0366	($547,199)
2/11/2019	Exercise of Options [*expiration date 12/21/2025*]	380,881	1/4 each on 9/8/2016; 9/8/2017; 9/8/2018; 9/8/2019	$14.6952	($5,597,122)
Sub-Total Options from Grants/Compensation				**Cost**	($0)
Sub-Total Options Exercised		413,000		**Cost**	($6,144,321)
RSU Transactions					
Transaction Date	**Unit Grants / Exercises**	**Units**	**Vesting Date**	**Price**	**Funds Spent / Gained**
2/9/2019	Exercise of RSUs	(61,289)	1/3 each on 12/29/2017; 2/9/2019; 2/9/2020	$0	$0
Sub-Total Grants of RSUs		(61,289)		**Cost**	($0)
Sub-Total Exercises of RSUs		0		**Proceeds**	$0
Stock Transactions					
Transaction Date	**Purchases / Sales**	**Shares**		**Price**	**Funds Spent / Gained**
2/9/2019	Acquired by RSUs exercise	61,289		$0	$0
2/9/2019	Sale	(27,419)		$56.6100	$1,552,190
2/11/2019	Acquired by options exercise	32,119		*See above*	*See above*

2/11/2019	Acquired by options exercise	380,881	*See above*	*See above*
2/11/2019	Sale	(158,795)	$57.8800	$9,191,055
2/11/2019	Sale	(254,205)	$57.5184	$14,621,460
Sub-Total Stock Sales		(440,419)	**Proceeds**	**$25,364,704**
Totals	**Shares Purchased**	**0**	**Transaction Costs**	**$0**
	Shares Acquired by Options Exercise	**413,000**	**Transaction Costs**	**($6,144,321)**
	Shares Acquired by RSU Exercise	**61,289**	**Transaction Costs**	**($0)**
	Shares Sold	**(440,419)**	**Transaction Proceeds**	**$25,364,704**
		Net Gain to Defendant Swidler		**$19,220,383**

176. These transactions during the Class Period, while the fraud was raging and the true facts regarding Match's business and operations, as alleged herein, remained hidden from investors, yielded the Defendant Ginsberg and Defendant Ginsberg a combined ***$35,559,961*** ($16,339,578 for Ginsberg, $19,220,383 for Swidler), along with 100,835 additional shares acquired at no or low expense (66,965 for Ginsberg, 33,870 for Swidler) in net ill-gotten gains from prices inflated by the fraud alleged herein. These transactions and proceeds constitute strong evidence of scienter.

177. Moreover, these transactions were suspicious in amount, a fact that further supports a strong scienter inference. For instance, Ginsberg's $16,339,578 in Class Period insider transaction gains compare suspiciously against her 2017 salary of $500,000 (or her $1,250,000 total compensation, including her $750,000 bonus) and her 2018 salary of $750,000 (or her

$2,500,000 total compensation, including her $1,750,000 bonus). Similarly, Swidler's $19,220,383 in Class Period insider transaction gains compare suspiciously against his 2017 salary of $550,000 (or his $1,800,000 total compensation, including his $1,300,000 bonus) and his 2018 salary of $550,000 (or his $2,000,000 total compensation, including his $1,500,000 bonus).

178. These transactions were also suspicious in timing vis-à-vis the alleged fraudulent misstatements and the alleged partial corrective disclosures, a fact that further supports the scienter inference. Even where the vesting date for RSUs or stock options had been pre-determined, Ginsberg and Swidler timed the misstatements and omission so as to inflate Match's stock price in the leadup to those vesting dates and timed Match's corrective disclosures to occur after a slate of transactions, thereby maximizing their net profits. For instance, the 2/6/2019 Form 8-K, 2/6/2019 Press Release, 2/6/2019 Article, 2/7/2019 Investor Call, and Ginsberg's 2/7/2019 Interview were all communicated just before Match's February 8, 2019 announcement of a $300 million offering, Ginsberg's and Swidler's February 9, 2019 RSU conversion, Swidler's February 11, 2019 options exercise, and Swidler's and Ginsberg's February 9-11, 2019 stock sales, which were followed shortly after by Match's disclosure of the FTC investigation on February 28, 2019. Ginsberg's other transactions follow similarly suspect patterns. For instance, Ginsberg's RSU conversions and stock sales on December 21, 20218 followed by less than one day her 12/20/2018 Interview and the 12/21/2018 Articles with excerpts of her interview and were preceded just a month prior by the misstatements in the 11/6/2018 Form 8-K, 11/6/2018 Press Release, 11/7/2018 Investor Call, and Q3 2019 Form 10-Q filed on November 9, 2018. Likewise, Ginsberg's May 30, 2019 options exercises and stock sales followed just a couple of weeks after the 5/7/2019 Form 8-K, 5/7/2019 Press Release, 5/8/2019 Investor Call, Ginsberg's 5/8/2019 Interview, Swidler's 5/8/2019 Interview, and the Q1 2019 Form 10-Q filed on May 9, 2019, and preceded by roughly

two months the corrective disclosures in early August 2019. Similarly, Ginsberg's December 21, 2019 RSU conversions and stock sales followed not only various misstatements in fall 2019, but also more recently the 11/5/2019 Form 8-K, 11/5/2019 Press Release, 11/6/20129 Investor Call, and Q3 2019 Form 10-Q filed on November 7, 2019, and occurred just before the January 31, 2020 twin announcements of a Congressional investigation and Ginsberg's resignation as Match CEO. Put differently, knowing the vesting dates of their RSUs and options, Ginsberg and Swidler repeatedly timed the misstatements alleged herein to maintain artificial inflation in Match's stock price before the exercise/sale dates and timed the corrective disclosures and events alleged herein to delay resulting stock declines until after their transactions, thereby wrongfully increasing and maximizing their net proceeds.

179. In addition, these transactions were suspicious in amount compared to pre-Class Period trading. For instance, as shown above, Swidler sold 440,419 shares during the Class Period for net proceeds of $19,220,383. By contrast, he sold 368,762 shares, for net proceeds of $15,492,392, during the same-length time period immediately preceding the Class Period. Thus, he sold nearly 20% more stock for over 24% higher net proceeds during the Class Period. Similarly, Ginsberg's Class Period net profits of $16,339,578 far outstripped her net proceeds from sales during the same-length time period immediately pre-Class Period, which totaled only $9,695,305, an increase of over 40%.

3. Defendants Ginsberg And Swidler Failed To Disclose One SEC Investigation And Two FTC Investigations While Insider Trading

180. Match was the subject of at least one undisclosed SEC investigation when the Defendants Ginsberg and Swidler were employed at Match and engaging in insider transactions. As revealed by a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. §552, an SEC investigation into "Financial Fraud/Issuer Discl" at Match was initiated May 16, 2016 and ended

January 3, 2017. Defendants did not disclose its existence, nature, or resolution to the market, whether in press releases, SEC filings, or otherwise. As discussed *supra*, Defendants delayed disclosure of the FTC investigation that resulting in a still-pending lawsuit being filed in September 2019 regarding the marketing of fraudulent accounts to entice non-paying users to subscribe. Pursuant to another FOIA request, Lead Plaintiffs uncovered another FTC investigatory subpoena dated March 8, 2019 and served on Match regarding its merger with Hinge, which the company likewise did not disclose to investors. The failure by Defendants Match, Ginsberg, and Swidler to promptly disclose these investigations to investors, particularly the one that led the FTC to sue over the marketing of fraudulent accounts – a topic at issue in many of the misstatements alleged herein – violated a duty to disclose, was a deception on investors, and evidences scienter.

4. Suspicious Resignations, Including By Defendant Ginsberg, Evidence Scienter

181. Another fact supporting a strong inference of scienter is the suspicious resignation of high-ranking executives, specifically Sam Yagan and Defendant Ginsberg, who were the only two members of Match's Board of Directors who worked at Match.com during the periods in which they would have had direct knowledge of the underlying misconduct described in the FTC's complaint, and Elie Seidman, Tinder's CEO during the Class Period.

182. In a September 24, 2019 8-K (the "9/24/19 8-K"), at the height of the fraud alleged herein and just a day before the FTC announced its lawsuit against Match.com, Match announced that Sam Yagan, who was the former CEO of Match and co-founder of OKCupid, resigned his position as Vice-Chairman of the Board of Directors of Match. The 9/24/19 8-K gave ***no reason*** for his resignation only stating that "it was not the result of any disagreement with the Company on any matter relating to the Company's operations, policies or practices."

183. As Defendants' fraud was revealed and the Class Period ended, in a January 31, 2020 8-K (the "1/31/20 8-K"), Match announced that Defendant Ginsberg was stepping down as CEO and member of the Board of Directors, effective March 1, 2020. The 1/31/20 8-K said Ginsberg's decision to resign "was not the result of any disagreement with the Company on any matter relating to the Company's operations, policies or practice." This resignation announcement was made the same day as a Congressional subcommittee issued a press release, as alleged herein, which announced an investigation into Match and three other dating apps regarding underage users, risks posed by registered sex offender and violent criminal users, and inappropriate selling or sharing of personal data and released a letter sent to Match requesting documents and information and requiring a responsive production by February 13, 2020. While Defendant Ginsberg did publicly disclose certain health issues, that they prompted her otherwise suspicious resignation is undermined by the fact that she joined the Board of Directors of Uber Technologies, Inc. just ***two weeks later*** in February 2020, the ***same month*** as she also joined the Board of Directors of Z-Work Acquisition Corp, while maintaining her membership on the Board of JC Penney Co., Inc. A year later, she added another Board position, joining the Board of thredUP on February 2, 2021.

184. Moreover, Ginsberg was permitted to retain her lavish executive compensation package, in exchange for nebulas advisory duties. The 1/31/20 8-K also stated that on January 29, 2020, Match entered into an agreement with Ginsberg, pursuant to which she would advise Match on matters relating to its business, strategy, and operations. According to the 1/31/20 8-K, pursuant to the terms of the agreement, which ended on February 28, 2021, Ginsberg's restricted stock units continued to vest, and her stock options remained exercisable and continued to vest, as applicable, as long as she continued to perform services for Match.

185. Thus, right as alleged fraud was being revealed, after an extended period of significant insider sales at inflated stock prices that netted her over $16 million in ill-gotten gains, Defendant Ginsberg resigned as CEO and moved to an "advisory role" that permitted continued vesting of her Match stock options, while she expanded her Board memberships in other companies. Defendant Ginsberg ensured protection for herself, while leaving Match's shareholders unprotected against stock declines caused by the revelation of Defendants' fraud.

186. Shortly after the Class Period, and while the FTD investigation remained pending, in July 2020, Tinder CEO Elie Seidman, also resigned and left the company.

5. The Fraud Implicated Core Operations

187. The fraud alleged herein implicates the core operations of Match. An overwhelming 98% of Match's total revenue is derived from direct revenue, which is primarily recurring subscriptions fees from its branded websites and apps. The alleged misconduct directly implicated the growth and quality of its subscriber base, Match's lifeline. High-level CWs have stated that the prevalence of fraud on Match's branded websites and apps ranged between 15% and 20% - or one out of every five or six users. Such a high rate of illegitimate accounts undermined the integrity of Match's reported metrics, including its PMC and ARPU, and put its bona fide members at risk. The underlying misconduct was serious enough for the FTC to open an investigation and, despite Defendants' denials of wrongdoing, file a complaint.

188. FTC statistics help quantify the extent of the problem. In February 2020, the FTC reported that 25,000 consumers reported losing $201 million to romance scams in 2019. This huge figure represents just a sliver of the activity of fraudsters on dating apps and websites – limited only to self-reported victims of successful, sufficiently large romance scams. The scale of fraudulent account activity is magnitudes larger. Match's corporate website has self-described

Tinder as the #1 downloaded dating app worldwide and the #1 grossing app overall worldwide. When added to Match's full portfolio of branded dating apps and websites, its dominant market share – recently estimated by *Vox* and *Business Insider* at 60% of the dating app market alone – renders Match's customers and its revenue streams uniquely vulnerable to the economic risks of fraudulent activity.

189. Given the foregoing, it is inconceivable that Defendants Ginsberg and Swidler, Match's CEO and CFO, the other Match senior executives discussed herein, and Match's Board of Directors did not know the facts and circumstances of the fraud as alleged herein. Moreover, such knowledge is imputable to Defendants Ginsberg and Swidler, given the implication of core operations, their roles and status within Match, and the litany of facts alleged herein regarding the funneling of information to them and their personal involvement in the key events and circumstances at issue, as alleged herein, including by the CW statements.

6. Defendants Ginsberg and Swidler Signed, Were Quoted In, or Sox Certified the Alleged Misstatements

190. As the individuals who signed, were quoted in, or orally made the alleged false and misleading statements described herein, Defendants Ginsberg and Swidler were under an obligation to familiarize themselves with the subject matter of those public statements and to speak truthfully. As alleged herein, they violated such duties.

191. As the individuals who SOX certified SEC filings as described above, Defendants Ginsberg and Swidler were obligated to inquire and investigate, familiarize themselves with the subject matter of their SOX certifications, and reassure themselves that the certifications were accurate and that they were speaking truthfully in making them. As alleged herein, they violated such duties.

192. When viewed holistically with the enhanced scienter allegations set forth herein, these facts support a strong inference of scienter for both Ginsberg and Swidler.

7. The Fraud And Retaliation Against Employees Violated Match's Corporate Code of Business Conduct and Ethics

193. Match's Code of Business Conduct and Ethics ("Code of Ethics"), published on its website throughout the Class Period, barred all the misconduct detailed by the extensive CW statements set forth above, as well as the insider trading alleged herein. By its express terms, the Code of Ethics applied to Defendants Ginsberg and Swidler throughout the Class Period. It stated, "This Code of Ethics applies to ***all Match Group*** directors, ***officers*** and employees, as well as to directors, officers and employees of each subsidiary of Match Group."

194. The Code of Ethics required Match, Ginsberg and Swidler to provide full and accurate disclosure in its SEC filings and all other public communications:

> ***The Company is committed to providing full, fair, accurate, timely and understandable disclosure in all reports and documents filed with or submitted to the Securities and Exchange Commission ("SEC") and in all other public communications made by the Company.***
>
> Any covered person who learns of any material information affecting or potentially affecting the accuracy or adequacy of the disclosures made by the Company in its SEC filings or other public statements shall bring the matter promptly to the attention of a member of the Match Group Disclosure Committee.
>
> * * * *
>
> Any covered person who learns of any information concerning: **…** (ii) any fraud, whether or not material, involving management or other employees who have a significant role in the Company's financial reporting, disclosures or internal controls, shall bring the matter promptly to the attention of a member of the Disclosure Committee.
>
> Upon receipt of any such information, the Disclosure Committee shall investigate the matter, consult with senior management as warranted, confer with the Audit Committee if appropriate, and ensure that any necessary corrective action is taken.

195. The Code of Ethics also makes clear that Match directors, officers, and employees (covered persons) were required to not only act lawfully, but also be honest and straightforward in its business dealings. The Code of Ethics states in relevant part:

> ***This Code of Business Conduct and Ethics [ ] reflects the commitment of Match Group, Inc. ("Match Group" and, together with its businesses, the "Company") to conduct its business affairs in accordance with not only the requirements of law, but also standards of ethical conduct that will maintain and foster the Company's reputation for honest and straightforward business dealings.***
>
> * * * *
>
> ***The conduct of covered persons in performing their duties on behalf of the Company must in all situations, as to all matters and at all times, be honest, lawful and in accordance with high ethical and professional standards.***

196. The Code of Ethics also prohibited retaliation of the kind suffered by CW9 and CW10, stating, "It is prohibited, and is a violation of this Code of Ethics, for anyone associated with the Company to retaliate in any way against anyone who has reported to the Company in good faith information indicating that a violation of this Code may have occurred or may be about to occur." It added, "Prohibited forms of retaliation include adverse employment actions (such as termination, suspension and demotion), the creation of a hostile work environment, and any other type of reprisal for the good-faith reporting of a possible violation of this Code of Ethics."

197. Match's Form 10-K filings during the Class Period, which directed investors to where the Code of Business Conduct was posted on Match's corporate website, stated, "The Company's code of ethics ***applies to all employees*** (***including Match Group's principal executive officer, principal financial officer,*** and principal accounting officer) and directors and is posted on the Company's website at http://ir.mtch.com under the heading of "Corporate Governance." By signing and SOX-certifying those Form 10-K filings, Defendants Ginsberg and Swidler *de*

facto expressly acknowledged review, receipt, understanding, and acceptance of the Code of Ethics and effectively declared their compliance and non-violation thereof.

198. In this context, Ginsberg's and Swidler's violation of express corporate policy further buttresses the inference of their scienter, whether based on their knowledge or their recklessness.

VI. NO SAFE HARBOR

199. The statutory safe harbor provided for forward-looking statements under certain circumstances does not apply to any of the allegedly false statements pleaded in this Complaint. Most, if not all, of the specific statements pleaded herein were not identified as "forward-looking statements" when made. To the extent any statements were labelled as forward-looking, they included statements of then-historical or then-present fact and there were no meaningful cautionary statements identifying important factors that could cause actual results to differ materially from those in the purportedly forward-looking statements. Any purported cautionary language warned only of theoretical future risks at times when those risks had already ripened due to Match's then-ongoing misconduct as alleged herein. Moreover, the purported cautionary language failed to adjust over time, using the same theoretical tone even after concrete changes of circumstance.

200. Alternatively, to the extent that the statutory safe harbor does apply to any forward-looking statements pleaded herein, Defendants are liable, because at the time each of those forward-looking statements were made, the particular speaker knew that the particular forward-looking statement was false, and/or the forward-looking statement was authorized and/or approved by one or both of the Individual Defendants or an executive officer of Match who knew that those statements were false when made.

201. For all these same reasons, the bespeaks caution doctrine likewise does not apply to shield Defendants from liability.

VII. LOSS CAUSATION/ECONOMIC LOSS

202. The market for Match shares was open, well-developed, and efficient at all relevant times. During the Class Period, as detailed herein, Defendants engaged in a course of conduct and a scheme to deceive the market that artificially inflated Match's share price and operated as a fraud or deceit on Class Period purchasers of Match shares by misrepresenting the material facts as detailed herein. As detailed above, at the end of the Class Period, when Defendants' prior misrepresentations became known to the public, through a series of corrective disclosures, the price of Match shares fell precipitously, as the prior artificial inflation came out. As a result of their purchases of Match shares during the Class Period, Plaintiff and the other Class members suffered economic loss, *i.e.*, damages, under the U.S. federal securities laws.

203. During the Class Period, Defendants presented a misleading picture of Match's financial condition, revenues, performance, and business prospects. Defendants' false and misleading statements had the intended effect and caused Match shares to trade at artificially inflated prices throughout the Class Period and until the truth was fully revealed to the market.

204. In response to the issuance of partially corrective disclosures on February 28, 2019, August 9, 2019, August 12, 2019, September 25, 2019, November 6, 2019, December 2, 2019, and January 31, 2020, the price of Match shares sharply dropped, on high volume, as detailed herein, thereby removing inflation from the price of Match shares, causing real economic loss to Plaintiff and the Class Members, investors who had purchased Match shares during the Class Period.

205. The decline was a direct and proximate result of the nature and extent of Defendants' fraud being revealed to investors and the market. The timing and magnitude of the

price decline in Match shares negates any inference that the loss suffered by Plaintiff and the other Class members was caused by changed market conditions, macroeconomic factors or Match-specific facts unrelated to Defendants' fraudulent conduct.

206. The economic loss, *i.e.*, damages, suffered by Plaintiff and other Class members was a direct and proximate result of Defendants' fraudulent scheme to artificially inflate Match's share price and the subsequent significant decline in the value of Match shares when Defendants' prior misrepresentations and other fraudulent conduct were revealed.

VIII. PRESUMPTION OF RELIANCE

207. At all relevant times, the market for Match shares was an efficient market, supporting a presumption of reliance under the fraud-on-the-market doctrine, for the following reasons, among others:

(a) Match met the requirements for listing, and was listed and actively traded on the NASDAQ under ticker symbol "MTCH", a highly efficient and automated market;

(b) Match had approximately 280.8 million shares outstanding as of December 31, 2019 such that its stock was liquid. During the Class Period, numerous shares of Match stock were traded on a daily basis, with moderate to heavy volume, demonstrating an active and broad market for Match stock and permitting a strong presumption of an efficient market;

(c) As a regulated issuer, Match filed periodic public reports with the SEC;

(d) Match regularly communicated with public investors via established market communication mechanisms, including regular disseminations of press releases on the national circuits of major newswire services and other wide-ranging public disclosures, such as communications with the financial press and other similar reporting services;

(e) Match was followed by several securities analysts employed by major brokerage firms who wrote reports that were distributed to the sales force and certain customers of their respective brokerage firms during the Class Period; and

(f) Unexpected material news about Match was rapidly reflected and incorporated into Match's stock price during the Class Period.

208. As a result of the foregoing, the market for Match shares promptly digested current information regarding Match from all publicly available sources and reflected such information in the price of its stock. Under these circumstances, all purchasers of Match stock during the Class Period suffered similar injury through their purchase of Match stock at artificially inflated prices and a presumption of reliance applies.

209. Alternatively, Plaintiff and the Class members are entitled to the presumption of reliance established by the Supreme Court in *Affiliated Ute Citizens of the State of Utah v. United States*, 406 U.S. 128, 92 S. Ct. 2430 (1972), as Defendants omitted material information in their Class Period statements in violation of a duty to disclose such information, as detailed above.

IX. PLAINTIFFS' CLASS ACTION ALLEGATIONS

210. Plaintiffs bring this action as a class action pursuant to Rules 23(a) and 23(b)(3) of the Federal Rules of Civil Procedure on behalf of a class consisting of all those who purchased Match's common stock during the Class Period, and who were damaged thereby (the "Class").

211. Excluded from the Class are Defendants, the officers and directors of Match at all relevant times, members and their immediate families and their legal representatives, affiliates, heirs, successors or assigns, and any entity in which Defendants have, or had, a controlling interest.

212. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, Match's common stock was actively traded on

NASDAQ. While the exact number of Class members is unknown to Plaintiffs at this time and can only be ascertained through appropriate discovery, Plaintiffs believe that there are hundreds or thousands of members in the proposed Class. Record owners and other members of the Class may be identified from records maintained by Match or its transfer agent and may be notified of the pendency of this action by mail, using the form of notice similar to that customarily used in securities class actions.

213. Plaintiffs' claims are typical of the claims of the members of the Class, since all members of the Class are similarly affected by Defendants' wrongful conduct in violation of federal law alleged herein.

214. Plaintiffs will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in class action and securities litigation.

215. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the questions of law and fact common to the Class are:

(a) whether Defendants' acts constituted violations of the federal securities laws;

(b) whether Defendants' statements made to the investing public during the Class Period misrepresented material facts concerning Match's business, operations, and financial condition;

(c) whether the Individual Defendants caused Match to issue false and misleading financial statements during the Class Period;

(d) whether Defendants acted knowingly or recklessly in issuing false and misleading financial statements;

(e) whether the price of Match's common stock was artificially inflated during the Class Period because of Defendants' conduct complained of herein; and

(f) whether members of the Class have sustained damages and, if so, what is the proper measure of damages.

216. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. Additionally, there will be no difficulty in the management of this action as a class action.

217. As alleged herein, Plaintiffs will rely, in part, on the presumption of reliance established by the fraud-on-the-market doctrine, inasmuch as Defendants made public misrepresentations or failed to disclose material facts during the Class Period; the misrepresentations and omissions were material and would tend to induce a reasonable investor to misjudge the value of Match's stock; and Plaintiffs and members of the Class purchased or otherwise acquired Match stock between the time the Defendants misrepresented or failed to disclose material facts and the time the true facts were disclosed, without knowledge of the omitted or misrepresented facts.

X. CLAIMS FOR RELIEF

COUNT I

Violation of Section 10(b) of the Exchange Act and SEC Rule 10b-5 Promulgated Thereunder Against All Defendants

218. Plaintiff repeats and realleges each and every allegation contained above as though set forth in full herein.

219. This Count is asserted against Defendants and is based upon Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder by the SEC.

220. During the Class Period, Defendants engaged in a plan, scheme, conspiracy and course of conduct, pursuant to which they knowingly or recklessly engaged in acts, transactions, practices and courses of business which operated as a fraud and deceit upon Plaintiffs and the other members of the Class; made various untrue statements of material facts and omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and employed devices, schemes and artifices to defraud in connection with the purchase and sale of securities. Such scheme was intended to, and, throughout the Class Period, did: (i) deceive the investing public, including Plaintiffs and other Class members, as alleged herein; (ii) artificially inflate and maintain the market price of Match common stock; and (iii) cause Plaintiffs and other members of the Class to purchase or otherwise acquire Match stock and options at artificially inflated prices. In furtherance of this unlawful scheme, plan and course of conduct, Defendants, and each of them, took the actions set forth herein.

221. Pursuant to the above plan, scheme, conspiracy and course of conduct, each of the Defendants participated directly or indirectly in the preparation and/or issuance of the quarterly and annual reports, SEC filings, press releases and other documents and statements described above, including statements made to securities analysts and the media that were designed to influence the market for Match stock. Such reports, filings, releases and statements were materially false and misleading in that they failed to disclose material adverse information and misrepresented the truth about Match's operations, finances and business prospects.

222. Defendants had actual knowledge of the materially false and misleading statements and material omissions alleged herein, including by virtue of their positions at Match,

and intended thereby to deceive Plaintiffs and the other members of the Class, or, in the alternative, Defendants acted with reckless disregard for the truth in that they failed or refused to ascertain and disclose such facts as would reveal the materially false and misleading nature of the statements made, although such facts were readily available to Defendants. Said acts and omissions of Defendants were committed willfully or with reckless disregard for the truth. In addition, each Defendant knew or recklessly disregarded that material facts were being misrepresented or omitted as described above.

223. Defendants were personally motivated to make false statements and omit material information necessary to make the statements not misleading in order to personally benefit from the sale of Match stock.

224. Information showing that Defendants acted knowingly or with reckless disregard for the truth is peculiarly within Defendants' knowledge and control. Defendants' first-hand knowledge is alleged herein. Moreover, as the senior managers and/or directors of Match, the Individual Defendants had knowledge of the details of Match's operations, business, and internal affairs.

225. The Individual Defendants are liable both directly and indirectly for the wrongs complained of herein. Because of their positions of control and authority, the Individual Defendants were able to and did, directly or indirectly, control the content of the statements of Match. As officers and/or directors of a publicly held company, the Individual Defendants had a duty to disseminate timely, accurate, and truthful information with respect to Match's businesses, operations, financial condition and prospects. As a result of the dissemination of the aforementioned false and misleading reports, releases and public statements, the market price of Match stock was artificially inflated throughout the Class Period. In ignorance of the adverse facts

concerning Match's business, operations and financial condition concealed by Defendants, Plaintiffs and the other members of the Class purchased or otherwise acquired Match stock at artificially inflated prices and relied upon the price of the securities, the integrity of the market for the securities and/or upon statements disseminated by Defendants, and were damaged thereby.

226. During the Class Period, Match stock was traded on an active and efficient market. Plaintiffs and the other members of the Class, relying on the materially false and misleading statements described herein, which the Defendants made, issued or caused to be disseminated, or relying upon the integrity of the market, purchased or otherwise acquired shares of Match stock at prices artificially inflated by Defendants' wrongful conduct. Had Plaintiffs and the other members of the Class known the truth, they would not have purchased or otherwise acquired said securities or would not have purchased or otherwise acquired them at the inflated prices that were paid. At the time of the purchases and/or acquisitions by Plaintiffs and the Class, the true value of Match stock was substantially lower than the prices paid by Plaintiffs and the other members of the Class. The market price of Match stock declined sharply upon public disclosure of the fraud alleged herein, to the injury of Plaintiffs and Class members.

227. By reason of the conduct alleged herein, Defendants knowingly or recklessly, directly or indirectly, have violated Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder.

228. As a direct and proximate result of Defendants' wrongful conduct, Plaintiffs and the other members of the Class suffered damages in connection with their respective purchases, acquisitions, and sales of Match's securities during the Class Period, upon the disclosure that Match had been disseminating materially misstatements and omissions to the investing public.

COUNT II

Violation of Section 20(a) Of The Exchange Act Against the Individual Defendants

229. Plaintiffs repeat and reallege each and every allegation contained above as though set forth in full herein.

230. During the Class Period, the Individual Defendants participated in the operation and management of Match, and conducted and participated, directly and indirectly, in the conduct of Match's business affairs. Because of their senior positions, they knew the adverse non-public information about Match's business, operations, finances, and prospects.

231. As officers and/or directors of a publicly owned company, the Individual Defendants had a duty to disseminate accurate and truthful information with respect to Match's business, operations, financial condition, results of operations, and prospects and to correct promptly any public statements issued by Match which had become materially false or misleading.

232. Because of their positions of control and authority as senior officers and directors, the Individual Defendants were able to, and did, control the contents of the various reports, press releases and public filings which Match disseminated in the marketplace during the Class Period concerning Match's business, operations, financial condition, results of operations, and prospects. Throughout the Class Period, the Individual Defendants exercised their power and authority to cause Match to engage in the wrongful acts complained of herein. The Individual Defendants, therefore, were "controlling persons" of Match within the meaning of Section 20(a) of the Exchange Act. In this capacity, they participated in the unlawful conduct alleged which artificially inflated the market price of Match stock.

233. Each of the Individual Defendants, therefore, acted as a controlling person of Match. By reason of their senior management positions and/or being directors of Match, each of

the Individual Defendants had the power to direct the actions of, and exercised the same to cause, Match to engage in the unlawful acts and conduct complained of herein. Each of the Individual Defendants exercised control over the general operations and business of Match and possessed the power to control the specific activities that comprise the primary violations about which Plaintiffs and the other members of the Class complain.

234. By reason of the above conduct, the Individual Defendants are liable pursuant to Section 20(a) of the Exchange Act for the violations committed by Match.

XI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief and judgment, as follows:

A. Determining that this action is a proper class action under Rule 23 of the Federal Rules of Civil Procedure, and certifying Plaintiffs as a Class representatives;

B. Awarding damages in favor of Plaintiffs and the other Class members against all Defendants, jointly and severally, for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including prejudgment and post-judgment interest thereon;

C. Awarding Plaintiffs and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

D. Awarding such other and further relief as the Court may deem just and proper.

XII. DEMAND FOR TRIAL BY JURY

Plaintiffs hereby demand a trial by jury.

Dated: April 23, 2021

Respectfully submitted,

/s/ Matthew L. Tuccillo
Matthew L. Tuccillo

POMERANTZ LLP
Jeremy A. Lieberman (admitted *pro hac vice*)
Matthew L. Tuccillo (admitted *pro hac vice*)
Jennifer B. Sobers (admitted *pro hac vice*)
600 Third Avenue, 20th Floor
New York, NY 10016
Telephone: (212) 661-1100
Facsimile: (212) 661-8665
Email: jalieberman@pomlaw.com
Email: mltuccillo@pomlaw.com
Email: jbsobers@pomlaw.com

Counsel for Samir Ali Cherif Benouis and Co-Lead Counsel for the Class

GLANCY PRONGAY & MURRAY LLP
Ex Kano S. Sams II
Charles H. Linehan
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: (310) 201-9150
Facsimile: (310) 201-9160
Email: esams@glancylaw.com
Email: clinehan@glancylaw.com

Counsel for Phillip R. Crutchfield and Co-Lead Counsel for the Class

Joe Kendall
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 1450
Dallas, Texas 75219
Telephone: (214) 744-3000
Facsimile: (214) 744-3015
Email: jkendall@kendalllawgroup.com

Local Counsel for the Class

EXHIBIT A-3

United States District Court

NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

PHILLIP R. CRUTCHFIELD, Individually and on Behalf of All Others Similarly Situated	§	
v.	§	CIVIL ACTION NO. 3:19-CV-2356-S
MATCH GROUP, INC., AMANDA W. GINSBERG, and GARY SWIDLER	§	

ORDER

This Order addresses Defendants' Motion to Dismiss Second Amended Complaint ("Motion to Dismiss") [ECF No. 54]. The Court has reviewed Plaintiffs' Second Amended Class Action Complaint for Violations of the Federal Securities Laws ("Second Amended Complaint") [ECF No. 51], the Motion to Dismiss and its accompanying exhibits [ECF No. 55], Plaintiffs' Opposition to Defendants' Motion to Dismiss [ECF No. 58], and Defendants' Reply in Support of Motion to Dismiss Second Amended Complaint [ECF No. 62].

To defeat a motion to dismiss filed pursuant to Federal Rule of Civil Procedure 12(b)(6), a plaintiff must "plead enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp v. Twombly*, 550 U.S. 544, 570 (2007); *see also Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The Court must accept well-pleaded facts as true and view them in the light most favorable to the plaintiff. *Sonnier v. State Farm Mut. Auto Ins. Co.*, 509 F.3d 673, 675 (5th Cir. 2007). Because the Second Amended Complaint alleges securities fraud, Plaintiffs must also "state with particularity the circumstances constituting fraud," FED. R. CIV. P. 9(b), and must comply with the strictures imposed by the Private Securities Litigation Reform Act ("PSLRA"), *see* 15 U.S.C. § 78u-4(b). "The PSLRA has raised the pleading bar even higher and enhances Rule 9(b)'s particularity requirement for pleading fraud in two ways." *Neiman v. Bulmahn*, 854 F.3d 741, 746

(5th Cir. 2017) (quoting *Local 731 I.B. of T. Excavators & Pavers Pension Tr. Fund v. Diodes, Inc.*, 810 F.3d 951, 956 (5th Cir. 2016)). "First, the plaintiff must specify each statement alleged to have been misleading." *Id.* (internal quotation marks and citation omitted); *see also* 15 U.S.C. § 78u-4(b)(1). "Second, for each act or omission alleged to be false or misleading, plaintiffs must state with particularity facts giving rise to a strong inference that the defendant acted with the requisite state of mind." *Neiman*, 854 F.3d at 746 (internal quotation marks and citation omitted); *see also* 15 U.S.C. § 78u-4(b)(2)(A).

The Court has carefully scrutinized all 164 pages of the Second Amended Complaint, which contain extensive allegations addressing pleading deficiencies identified in the Court's Memorandum Opinion and Order [ECF No. 50]. Applying the standards of *Twombly* and *Iqbal*, as well as the PSLRA's heightened particularity requirement, the Court finds that Plaintiffs have adequately specified at least some allegedly misleading statements or omissions. The Court further finds that though Plaintiffs have pleaded the requisite inference of scienter for surviving a motion to dismiss, the Court anticipates that it will revisit this issue at a later phase in the litigation after discovery takes place.

Accordingly, dismissal is not warranted at this time and the Court **DENIES** the Defendants' Motion to Dismiss Second Amended Complaint.

SO ORDERED.

SIGNED November 19, 2021.

KAREN GREN SCHOLER
UNITED STATES DISTRICT JUDGE